www.monitor.co.at

11 Nov. 07

monitor

Das Magazin für Informationstechnologie

Risiko vermeiden Sicherheit erhöhen

Auf über 30 Seiten widmet sich diese Ausgabe den Themen IT-Risikomanagement und Sicherheitsoptimierung. Denn IT-Produkte, IT-Prozesse und IT-Projekte sind aufgrund der hohen Komplexität sowie der zu beachtenden zahlreichen Einflussfaktoren nicht frei von Risiken und so großen Unsicherheiten unterworfen.

- **MONITOR-Diskussion: IT-Consulter**
- **Job Training:** IKT-Ausbildung in Österreich, Teil 2
- **Marktüberblick:** USV-Anlagen

LOOK AT IT
Seite 30

Hier sollte Ihr Name stehen. Fragen Sie uns nach einem Abo. Tel. 01 | 74095-466

ISSN 1021-271X P.B.B. ZUL.NR. 02Z031040M – VERLAGSORT WIEN, VERLAGSPOSTAMT 1110 WIEN

We make sure

FUJITSU COMPUTERS SIEMENS

Wäre doch alles so problemlos wie Ihre IT.

Auf IT-Infrastrukturlösungen von Fujitsu Siemens Computers können Sie sich verlassen.

x10sure™ z. B. mit PRIMERGY RX300 Servern und leistungsstarken Intel® Xeon® Quadcore-Prozessoren sorgt dafür, dass sich bei einem Ausfall die betroffene Anwendung einfach auf einem Ersatzserver neu startet. Und weil sich mehrere produktive Systeme ein Ersatzsystem teilen, bietet x10sure™ eine hohe Ausfallsicherheit zu niedrigen Kosten. So können auch Unternehmen mit kleinen IT-Budgets von den Vorzügen einer professionellen Verfügbarkeitslösung profitieren. Und während die IT rund läuft, können Sie sich voll auf Ihr Geschäft konzentrieren.

Weitere Informationen erhalten Sie unter:
www.fujitsu-siemens.at oder unter 800 23 24 11 (zum Ortstarif)

intel
Xeon® inside™
Quad-core.
Unmatched.

Celeron, Celeron Inside, Centrino, Centrino Logo, Core Inside, Intel, Intel Logo, Intel Core, Intel Inside, Intel Inside Logo, Intel Viiv, Intel vPro, Itanium, Itanium Inside, Pentium, Pentium Inside, Xeon und Xeon Inside sind Marken der Intel Corporation in den USA und anderen Ländern.

Sicher ist sicher

Das Thema Sicherheit beschäftigt IT-Verantwortliche wie Geschäftsführer in Unternehmen in weiter steigendem Maße. Während nämlich gesetzliche Regelungen zunehmend strenger formuliert werden, ergibt sich gleichzeitig ein schwer überschaubares Gefahren-Szenario durch die wachsende Zahl weit verstreuter Benutzer und Endgeräte. Das Thema dieser Ausgabe bringt Sie daher auf den neuesten Sicherheitsstand.

Dipl.-Ing. Rüdiger Maier, Chefredakteur

Die jährliche Security Roadshow des IT-Marktforschers IDC gilt als Trendbarometer in Sachen IT-Sicherheit. Daher mischte sich MONITOR-Autor Alexander Hackl unter die rund 150 IT-Verantwortlichen aus österreichischen Unternehmen und verfolgte deren Diskussion mit den anwesenden Anbietern von IT-Sicherheitslösungen über Bedrohungen, Strategien und mögliche Auswege. Klar wurde dabei einmal mehr, dass das Thema bei IT-Verantwortlichen nach wie vor höchste Priorität genießt. Dazu IDC-Österreich-Geschäftsführer Joachim Seidler: „Der Security-Markt boomt weiterhin. Wir prognostizieren global ein jährliches Wachstum für Security-Services von 18,9% für die nächsten fünf Jahre, in Westeuropa steigt der Geschäftsbereich der Managed Security Services jährlich um 21,3% bis 2011."

Aber bereits an der Frage, ob die wachsenden Sicherheitsbudgets auch richtig angelegt werden, scheiden sich die Geister. Macht mehr Security ein Unternehmen ganz automatisch sicherer? Bjarne Kaiser Lauritzen, Europa-Vizepräsident des Netzwerk-Equipment-Anbieters Juniper, beantwortet die Frage im MONITOR-Gespräch schlichtweg mit „Nein". Ein Grundschutz mit Firewalls, Virenabwehr und Co sei zwar erforderlich, aber den hätten die meisten Firmen ohnehin. „Die größte Gefahr geht von leichtsinnigen Benutzern aus. Nach wie vor sind viele Firmen-PCs mit Passwörtern auf gelben Post-its vollgeklebt. Und nicht selten geben sich Hacker am Telefon als Support-Mitarbeiter aus, erfragen Passwörter und bekommen bereitwillig Auskunft." Verfolgen Sie die spannende Sicherheitsdiskussion ab Seite 24.

Risikomanagement in der IT

Einen umfassenden Blick auf die in der IT verborgenen Risiken wirft der Buch- und MONITOR-Autor Ernst Tiemeyer. Er stellt fest, dass IT-Produkte, Prozesse und Projekte aufgrund der hohen Komplexität sowie der zu beachtenden zahlreichen Einflussfaktoren nicht frei von Risiken und so großen Unsicherheiten unterworfen sind. Angefangen vom menschlichen Versagen bis zur fehlenden Kontrolle können sich negative Einflussfaktoren zu großen Problemen summieren. Für die Handhabung von IT-Risiken sind inzwischen allerdings auch einige hilfreiche und für die Praxis unverzichtbare Lösungsansätze entwickelt worden, die erhebliche Potenziale zur Zukunftssicherung eröffnen. Immer noch steht aber die Mehrheit der Unternehmen heute vor der Herausforderung, ein Risikomanagement-System für den IT-Bereich neu aufzusetzen oder grundlegend zu erweitern. Lesen Sie mehr über die Schritte hin zum funktionierenden Risiko-Management ab Seite 12.

Komplexität der IT: Berater freuen sich

Nach der Krise 2002/2003 ist der IT-Berater-Markt in Österreich wieder gut erholt. Immer raschere Produktzyklen, der Innovationsdruck sowie die Komplexität der IT-Architektur und -Applikationen verhelfen ihnen zu vollen Auftragsbüchern. Grund genug für MONITOR, Mitte Oktober eine Expertenrunde zum Thema „Aktuelle Trends und Herausforderungen in der IT-Beratung" zu versammeln. MONITOR-Autorin Christine Wahlmüller fasst ab Seite 46 die Ergebnisse der unter meiner Leitung sehr angeregt diskutierenden Runde zusammen.

Immer mehr Unternehmen erkennen, dass mit einer optimierten IT die Geschäftsprozesse besser laufen. Mit diesem Ziel werden gerne IT-Berater zu Hilfe geholt. Aber: Oft vernachlässigte Grundvoraussetzung für eine erfolgreiche Beratung ist das wechselseitige Verständnis von Management und Fachabteilungen einerseits und der internen IT-Abteilung sowie externen Beratern andererseits. Die hauseigene IT wird laut aktuellen Studien sogar als Wachstumsbremser gesehen und beschert nach Meinung der Manager den Unternehmen durchschnittlich 5% weniger Umsatzwachstum. Um nicht nur theoretisch zu diskutieren, war mit Anton Leitner der IT-Leiter der NÖM AG anwesend. Er war früher selbst IT-Berater bei Capgemini und Spezialist für die Einführung von SAP, kennt also beide Seiten: „Früher, noch vor zehn Jahren, waren wir die Götter, und in den Unternehmen gab es wenig Wissen über SAP. Heute, vor allem nach dem Crash der Branche 2002, hat sich das Bild sehr gewandelt."

Fachhochschulen: Vielfältiges Angebot in der IKT-Ausbildung

Das Ausbildungsangebot im Bereich Informationstechnologie (IT) oder Telekommunikation (TK) ist vielfältig wie noch nie. Waren im ersten Teil der MONITOR-Serie (Heft 9) die österreichischen Universitäten an der Reihe, so berichtet MONITOR-Autorin Christine Wahlmüller im zweiten Teil unserer vierteiligen Serie über alle IT/TK-Studiengänge der Fachhochschulen in Wien, Niederösterreich, Burgenland und in der Steiermark.

Eine interessante und anregende Lektüre wünscht Ihnen Ihr

Inhalt | November 2007

Wirtschaft

Vorschau: ITnT 2008 6
REBOOT 8

Lösungen

Konica Minolta & Erste Bank: Papier-Output-Management 10

Thema | Security

IT-Risikomanagement: Aktuelle Herausforderungen, Instrumente, organisatorische Lösungen 12
Microsoft Security: Sicherheit mit Vista 16
Sicheres Exchange Publishing 18
IT-Security-Lösung in den Constantin Kinos 19
Smartcards bei Energie AG 22
Jenseits von Gut und Böse: Aktuelle IDC-Security-Trends 24
„Der Mitbewerb tut sich schwer mit uns." - Interview mit Wieland Alge, CEO phion 27
Nachlese: schoeller network control Forum 2007 28
„Mehr Compliance, mehr Sicherheit" 30
Bänderriss - wie Daten gerettet werden können 32
Sicherheitsbewusstsein kann man lernen 34
Marktübersicht: USV-Anlagen 38
Sicherheit für Webanwendungen 39
Österreichische Privatbank setzt auf NOD32 41
Moderne Verschlüsselungsmethoden 43

Strategien

„Mobility Award 2007" 45
MONITOR-Diskussion: Komplexität der IT beschert IT-Beratern Hochkonjunktur 46

Job Training

IKT-Ausbildung in Österreich, Teil 2: Praxisorientiert und schnell zu Wissen und Titel 50
Die FH-IT-Studiengänge auf einen Blick 51

Netz & Telekom

NetApp Innovation 2007 56
KSI: Maßstab für eine robuste Netzwerk-Infrastruktur 57
Erwartungen an ein völlig neues Internet 58

Hard & Software

Maxdata: Neue Strategie 60
Neue Multifunktionsgeräte 61
Universal-Ladegerät 62

Aus der Redaktion

Editorial 3
Inserentenverzeichnis 63
Impressum 63

IT-Risikomanagement: Aktuelle Herausforderungen, Instrumente, organisatorische Lösungen

MONITOR-Diskussion: Hochkonjunktur bei IT-Beratern

you can

Canon

Wecken Sie Ihre Kreativität – mit den PIXMA All-in-One-Geräten von Canon. Erschaffen Sie sich Ihre eigene Welt mit Features wie intelligente Kopierfunktionen, detailreiches Scannen und Fotodruck in herausragender Qualität. Die Quick-Start-Funktion sorgt dafür, dass Sie gleich loslegen können und das Easy-Scroll-Bedienrad macht die Bedienung spielend einfach. Lassen Sie sich inspirieren: **www.canon.at/pixma**

PIXMA

Meine Freiheit

Vorschau: ITnT 2008

Österreichs größte Fachmesse für Informationstechnologie und Telekommunikation findet vom 5. bis zum 7. Februar 2008 statt.

„Die ITnT ist ein starker Impulsgeber der IKT-Branche in Österreich und im zentral-, süd- und osteuropäischen Raum." - DI **Matthias Limbeck**, Reed Exhibitions Messe Wien

Die Messe gilt inzwischen als wichtige Plattform sowohl für den heimischen als auch für den IKT-Markt in den mittel-, ost- und südosteuropäischen Ländern (CEE/SEE).

Als reine B2B-Veranstaltung beruht sie auf drei thematischen Schwerpunkten: „Infrastructure & Solutions", „Software & Services" sowie „Telecommunications & Solutions". Ergänzt wird sie durch ein umfangreiches Rahmenprogramm wie auch zielgerichteten Networking-Veranstaltungen.

Im Vorjahr gab es, so Veranstalter Reed Exhibitions Messe Wien, 389 Aussteller und 16.874 Besucher. „Die ITnT entwickelt sich entgegen dem allgemeinen Trend bei internationalen IT-Fachmessen sehr positiv und bleibt weiterhin auf Erfolgskurs", freut sich Matthias Limbeck, themenverantwortlicher Geschäftsführer bei Reed Exhibitions Messe Wien.

Neben Ausstellungen und Präsentationen stehen rund 80 Vorträge, Seminare und Podiumsgespräche am Programm der ITnT 2008. Dazu kommen Networking-Termine sowohl untertags als auch abends. „Ein umfangreiches Rahmenprogramm und Networking-Plattformen zum Kontaktknüpfen und -pflegen gehören ebenso zu einer modernen Fachmesse wie die klassische Ausstellung der Produkte und Dienstleistungen", unterstreicht Reed-Messeleiter Mag. Günter Theuermann.

Die Bedeutung der ITnT im internationalen Umfeld soll ebenfalls gesteigert werden. So nahmen 2007 zum Beispiel 18 Firmen aus der Tschechischen Republik teil und präsentierten IKT-Lösungen und -Dienstleistungen.

Die Schweiz, unter dem Dach der Handelskammer Schweiz-Österreich und Liechtenstein, wird den Auftritt bei der ITnT 2008 im Vergleich zu 2007 vergrößern.

www.itnt.at

Edmund Haberbusch zu ACP

Edmund Haberbusch tritt in die Geschäftsleitung von ACP ein.

Neues Mitglied der Geschäftsleitung bei ACP: **Edmund Haberbusch**

Haberbusch, 50, übernimmt bei ACP den Bereich Produktmanagement und Technik für Österreich und Deutschland. Er kommt von der Telekom Austria, wo er zuletzt das Produkt-Management und Produktmarketing für die Geschäftskunden leitete und damit für 50 Mitarbeiter und 300 Mio. Euro Umsatz verantwortlich war.

Mit Produktmanagement & Technik schuf man bei ACP eine neue Position, um das Serviceangebot in der Gruppe schlagkräftig zu bündeln. Haberbusch wird das Produktportfolio von ACP über die Grenzen hinweg standardisieren und das Serviceangebot ausweiten. „Der Trend bei den Unternehmen geht in die Richtung, sich auf die eigene Kernkompetenz zu konzentrieren und alle anderen Leistungen extern zuzukaufen", schildert Haberbusch. „Für ACP als großes Systemhaus bietet das beträchtliche Wachstumschancen, und die will ich nutzen."

Karriere

Walter Weihs, 57, Vorstand der Software AG Österreich hat mit Anfang Oktober auch die Verantwortung für die Bestandskunden in der Schweiz übernommen. Walter Weihs steht seit dem Jahr 2000 an der Spitze der Software AG Österreich.

Herbert Dorner, 37, wurde zum Leiter der Abteilung Consulting & System Engineering bei S&T Austria bestellt. In dieser Position zeichnet er verantwortlich für die Beratung und Realisierung von IT-Projekten für Kunden in ganz Österreich. Dorner war zuletzt im Management von Microsoft tätig, davor als Produktmanager bei Navision Österreich.

Oliver Breithut, 37, übernimmt die Leitung des Bereichs IT Service Management (ITSM) der Softlab GmbH Wien und wird damit auch Mitglied der Geschäftsführung. Zugleich wurde das ITSM-Team als eigenständiger Geschäftsbereich aufgewertet. Breithut ist seit 1999 für die Softlab GmbH Wien tätig.

Dr. **Christian Büll**, 44, ist neuer Sales Director bei Sage bäurer und übernimmt die Gesamtverantwortung für die vertrieblichen Aktivitäten in Deutschland und Österreich. Er wird weiterhin auch als Vorsitzender der Geschäftsführung der österreichischen Tochtergesellschaft von Sage bäurer in Wien tätig sein.

Mag. **Birgit Gruber**, 27, ist neue Marketingmanagerin beim CRM-Spezialisten update software AG. Gruber verantwortet das komplette Marketing in Österreich und der Schweiz sowie das Marketing im Bereich Financial Services International. Zuletzt leitete sie die Bereiche CRM und Direktmarketing bei der Konica Minolta Business Solutions Austria GmbH.

Eine neue Perspektive für Ihr Geschäft?

Dem digitalen Auflagendruck gehört die Zukunft. Jetzt ist der Zeitpunkt, Ihrem Geschäft eine richtungsweisende Perspektive zu geben. Mit Digitaltechnik, die selbst Offsetverwöhnte überzeugt. Mit Workflow-Lösungen, die Ihre Arbeit radikal beschleunigen. Und mit einem Service, auf den Sie sich ohne Wenn und Aber verlassen können. Kurz: mit einem Partner, der Sie dabei unterstützt, neue Einnahmequellen zu erschließen.

Weitere interessante Perspektiven unter:
www.canon.at/imagePRESS

you can
Canon

imagePRESS C7000VP

Workflow
PROGRAM

Essential
Business
Builder
Program

UEFA
EURO2008
Austria-Switzerland

Offizieller Sponsor
der UEFA EURO 2008™

SAP Österreich: Neuer Managing Director

Mit Wirkung zum 1. Januar 2008 übernimmt Benno F. Weißmann die Position des Managing Director für SAP Österreich.

Benno F. Weißmann, SAP Österreich

In seiner neuen Rolle zeichnet Benno F. Weißmann verantwortlich für die strategische Planung sowie das operative Geschäft inklusive Vertrieb, Services und Support der SAP in Österreich. Weißmann berichtet an Ferri Abolhassan, Executive Vice President Large Enterprise EMEA, Mitglied des EMEA Executive Regional Leadership Teams und in dieser Rolle verantwortlich für SAP in Algerien, Deutschland, Frankreich, Großbritannien und Irland, Österreich, Russland und GUS, die Schweiz sowie Skandinavien.

Weißmann folgt auf Wolfgang Schuckert, der SAP am Jahresende verlässt, um sich neuen Aufgaben zu widmen.

In seiner bisherigen Rolle als Vertriebsleiter und Mitglied der österreichischen Geschäftsführung von SAP hat Weißmann wesentlich zum Wachstum und der Profitabilität der gesamten Region beigetragen. Weißmann ist seit neun Jahren bei SAP in verschiedenen Vertriebs- und leitenden Partnermanagement-Funktionen tätig.

„Weißmann kennt nicht nur den Markt in Österreich sehr genau, er ist auch aufgrund seiner großen Erfahrung für diese neue Rolle bestens gerüstet", kommentiert Ferri Abolhassan.

Neuer CEO bei One

Seit Anfang Oktober hat One nicht nur neue Eigentümer, sondern auch einen neuen CEO.

Michael Krammer, One CEO.

Michael Krammer, 47, übernimmt die Position von seinem Vorgänger Jørgen Bang-Jensen, der zehn Jahre an der Spitze des drittgrößten österreichischen Mobilfunkbetreibers stand. Neben seiner Funktion als CEO wird Krammer interimistisch auch für die Marketing- und Vertriebsagenden von One verantwortlich sein.

Krammer ist in der österreichischen Telekom-Szene kein Unbekannter, war er doch CEO bei tele.ring. Für die Werbekampagne „Weg mit dem Speck" erhielt er mehrere Auszeichnungen, unter anderem die des Marketer des Jahres 2003.

Nach der Übernahme von tele.ring durch T-Mobile ging Krammer im Mai 2006 für ein Jahr als Vorsitzender der Geschäftsführung zu E-Plus nach Deutschland. Für die Position des CFO konnte Christian Fuchs, 43, gewonnen werden. Auch er kommt von tele.ring.

Mit Stichtag 2. Oktober 2007 haben der Finanzinvestor Mid Europa Partners 65% und die France-Telecom-Tochter Orange 35% der Anteile an One übernommen. Damit wurden die langjährigen Spekulationen um die Eigentümerstruktur des Mobilfunkers beendet.

REBOOT

Als sich die Hersteller von Security-Software vor einigen Jahren sehr stark in Szene setzten, zweifelte die Branche noch an der Notwendigkeit übertriebener Vorsicht im Computing. Heute sieht die Sache anders aus.

Conrad Gruber

Man erinnert sich an die vollmundigen Vorhersagen: Das IT-Security-Business werde in den kommenden Jahren ein Milliardenbusiness werden, tönten Marktforscher im Abklingen der Internet-Euphorie nach der Jahrtausendwende. Niemand mochte ihnen so recht glauben: Was sollte denn in IT-Netzwerken eine so große Bedrohung sein? Ein paar Software-Nerds, die Viren programmieren und Spam-Mails verschicken?

Heute wissen wir es besser: Spam ist zu einer Epidemie geworden, die nach neuesten Daten fast 90% (!) des weltweiten E-Mail-Verkehrs beansprucht. Die kleinen Computertüftler haben ausgedient, heute sind kriminelle IT-Spezialisten am Werk und bringen immer verfeinertere Schädlinge im Umlauf, nicht, um spaßhalber IT-Netzwerke zu stören, sondern um sich bewusst zu bereichern, mit all der kriminellen Energie, die dazu notwendig ist. Mailbombing, Phishing, Trojaner, Malware, Bakkdoor-Viren und so weiter bedrohen den IT-Alltag. Ohne mindestens eine Firewall und einen Virenscanner sollte man heutzutage wirklich keinen Computer, auch nicht den privaten, mehr einschalten. Vom komplexen IT-Netzwerken in Unternehmen ganz zu schweigen.

Die kriminelle Invasion in der IT bewirkt teure Schutzmaßnahmen und ist auch sonst hochgradig ärgerlich. Da vor allem die IT-Abteilungen in Unternehmen in höchstem Grade darauf erpicht sind, den Angreifern nur ja keine Hintertür offen zu lassen, werden E-Mail-Netzwerke behindert, Datentransfers blockiert, Logfiles mitgeschnitten und Spam auf riesige Mail-Server ausgelagert, weil man ja nie sicher sein kann, dass der Spamfilter nicht doch eine wichtige Nachricht unterschlagen hat.

IT-Security ist heute zum Computeralltag geworden. Zuletzt mischte sich auch der Staat ein und überlegt, ob er seine Bundesbürger nicht mittels Trojanern überwachen soll. Die zunehmende Mobility in Unternehmen eröffnet zusätzlich ein weites Feld, von dem man erst in Ansätzen erahnt, was da noch auf uns zukommt.

Erst kürzlich wurde wieder in Wien von WLAN-Piraten berichtet, die auf einer Tour durch die Stadt Hunderte von WLANs fanden, die offen standen wie die Scheunentore. Mobile Security, Data Protection, Persönlichkeitsschutz und Kopierschutz sind die Themen der Stunde. Tatsache ist, dass das Schaffen von Sicherheit immer komplexer wird: Das ist schlecht für den Anwender, aber gut für IT-Security-Spezialisten, deren Boom noch lange nicht zu Ende ist. ❑

MEHR SPEED FÜR IHR BUSINESS!

nur € 4.199,–*

*Unverbindliche Preisempfehlung in EUR inkl. MwSt.
MAXDATA ist ein international eingetragenes Warenzeichen. Intel, Intel Logo, Intel Core, Xeon, und Xeon Inside sind Marken der Intel Corporation oder ihrer Tochtergesellschaften in den USA oder anderen Ländern. Das Microsoft Logo ist ein eingetragenes Warenzeichen der Microsoft Corporation. Alle übrigen Markennamen können eingetragene Warenzeichen der jeweiligen Hersteller sein und sollen als solche betrachtet werden.

So geben Sie den Takt in Ihrem Business an. Aktuelle MAXDATA Server Hardware mit Intel® Xeon® Quadcore-Prozessoren verkürzt lästige Wartezeiten. So kann sich Ihre Mannschaft auf das Wesentliche konzentrieren.

Der MAXDATA PLATINUM 3200 I bringt Servertechnologie vom Feinsten. Er schöpft seine brachiale Leistung aus ganzen vier Prozessorkernen! Mit dem Intel® Xeon® Quadcore-Prozessor 5310 ist Ihr Server mit zwei Intel® Core™2 Duo Kernen nebeneinander ausgerichtet und bringt eine doppelte Leistung. Mit seiner Technik können Multi-Core-CPUs und 64-bit-Architekturen zeigen, was sie können. Performance und Sicherheit garantiert der Server darüber hinaus durch bis zu zehn Festplatten mit SAS-Unterstützung.

Performant - Sicher - Erweiterbar!

Setzen Sie in Sachen Server-Technology auf MAXDATA. Mehr dazu unter **www.maxdata.at** oder telefonisch unter **01/27789-0.**

MAXDATA
INDIVIDUALTECHNOLOGY

MAXDATA PLATINUM 3200 I: Intel® Xeon® Quadcore-Prozessor 5310 (1,60 GHz, 8 MB Cache), Intel® E5000P Chipsatz, 2 x 1 GB FB-DIMM 667 RAM mit ECC, 3 x 73 GB 15k hot swap SAS Festplatten (RAID 5 vorkonfiguriert), 6 hot swap Festplatteneinschübe, LSI870x ELP S-ATA/SAS RAID-Controller inkl. Battery Buffered Unit, DVD-ROM Laufwerk, Standgehäuse, 2 x 830 W redundante hot swap PFC Netzteile, redundante hot swap Lüfter, 3 x PCI Express x8, 1 x PCI Express x4, 2 x PCI 64 bit / 100 MHz, Remote Management Modul (Keyboard-Video-Maus Übertragung über LAN), DR DOS Preload, MAXDATA System Manager und MAXStart Installations-CD Software, 36 Monate Vor-Ort-Service am nächsten Arbeitstag

Konica Minolta setzt internationales Großprojekt für Erste Bank um

Umfassendes Soft- und Hardware-Paket optimiert Paper-Output-Management in Österreich und Osteuropa

Konica Minolta Business Solutions Austria gestaltet die Druck- und Kopier-Infrastruktur der Erste-Bank-Gruppe neu. Bei einem Auftragsvolumen im zweistelligen Millionen-Bereich werden sämtliche Paper-Output-Agenden in Österreich, Tschechien, Slowakei, Ungarn und Kroatien optimiert. Die Ausweitung des Projekts auf weitere Länder wie Rumänien und die Ukraine ist geplant.

Dabei kommen nicht nur fast 8.000 Drucker und Multifunktionsgeräte zum Einsatz. Wesentlicher Schwerpunkt des Projekts ist die mit den Multifunktionsgeräten (MFP) integrierte Software. „Es freut mich, dass wir in diesem internationalen Projekt neben unserer Hard- und Software vor allem auch mit unserem Lösungs-Know-how punkten konnten", sagt Johannes Bischof, Geschäftsführer Konica Minolta Business Solutions Austria.

Wichtigstes Ziel der Erste-Bank-Gruppe ist es, die Kosteneffizienz im Druck- und Kopierbereich deutlich zu steigern. „Im Rahmen einer gruppenweiten Ausschreibung konnte das Konzept von Konica Minolta mit den niedrigsten Druckkosten überzeugen. Gleichzeitig erwarten wir eine hohe Ausfallssicherheit und optimale Auslastung unserer Geräte", sind sich Ing. Kurt Essler, Geschäftsführer der s-DIS, eines Tochterunternehmens der Erste Bank für die dezentrale IT-Infrastruktur, und Dr. Gerald Schönwetter, Leiter des gruppenweiten Procurements für IT der Erste-Bank-Tochterfirma Procurement Services GmbH einig. Denn bisher hatte jedes Land eine eigene Gerätekultur mit unterschiedlichen Herstellern und einer Fülle von Modellen.

Weniger Drucker, mehr Komfort

Die bisherige historisch gewachsene Gerätevielfalt wird durch eine wesentlich kleinere Zahl von MFPs ersetzt. Das bedeutet, dass sich nunmehr - nach wirtschaftlichen Gesichtspunkten - mehr Mitarbeiter ein Gerät teilen als bisher. Zwei Software-Pakete machen dies ohne Komfort-Einbußen möglich:

„Follow-Me-Print" sorgt dafür, dass die Ausdrucke eines Mitarbeiters an dem Gerät herauskommen, in dessen Nähe er sich gerade befindet. Druckaufträge werden dazu solange am zentralen Printserver abgelegt, bis der Mitarbeiter sich durch PIN oder Karte bei einem der Drucker „meldet". So können die Mitarbeiter beinahe ortsunabhängig an jedem Multifunktionsgerät im gesamten Netzwerk drucken.

„Secure Print" schützt vertrauliche Dokumente. Der Ausdruck erfolgt auch hier erst, wenn der Mitarbeiter sich über Passwort oder Karte am Gerät identifiziert. So ist sichergestellt, dass sensible Dokumente wie Kostenvoranschläge auch in Papierform nur in die Hände des richtigen Mitarbeiters gelangen können.

Im täglichen Einsatz sorgen Remote-Service-Funktionen wie z. B. „iCare" für Komfort. So können beispielsweise dank eines integrierten GSM-Modems mit iCare ausgestattete Drucksysteme im Schadens- bzw. Problemfall selbsttätig professionelle Unterstützung durch einen Außendienstmitarbeiter von Konica Minolta rufen. Aber auch darüber hinausgehende Anwendungen wie Fernwartung, automatische Bestellung von Verbrauchsmaterial, die automatisierte Einhaltung von Serviceintervallen oder die Zählerstandsmeldung erleichtern den zuverlässigen Einsatz.

Dank weiterer Remote-Funktionen haben die Administratoren der Erste Bank stets den Überblick über die gesamte Druckerflotte. Webbasierte Server-Software lässt IT-Mitarbeiter alle Systeme zentral konfigurieren und überwachen. Automatisch generierte E-Mails informieren in Echtzeit über Probleme wie Papierstau oder Tonermangel.

Als Hardware kommen Konica-Minolta-Geräte zum Einsatz. Je nach Einsatzzweck nutzt die Erste-Bank-Gruppe die Multifunktionsgeräte C300, bizhub 250, bizhub 350 oder bizhub 420 sowie magicolor 2550, 5550 oder PagePro-1350-Drucker.

www.konicaminolta.at

firmenmonitor.at
Ein Service der Wiener Zeitung

++ Kunden- und Lieferantenmonitoring: Geschäftsführerwechsel + Konkurse +
Kapitalaufstockung + Insolvenzen + Firmenneugründung + Adressänderung +

Kommunikative wissen mehr!

firmenmonitor.at

Kostenlose Testaccounts und sämtliche Informationen unter www.firmenmonitor.at
oder unter der Service-Hotline (01) 206 99 – 600

+ E-Mail-Verständigung bei allen Änderungen + Tagesaktuell + Zuverlässig +

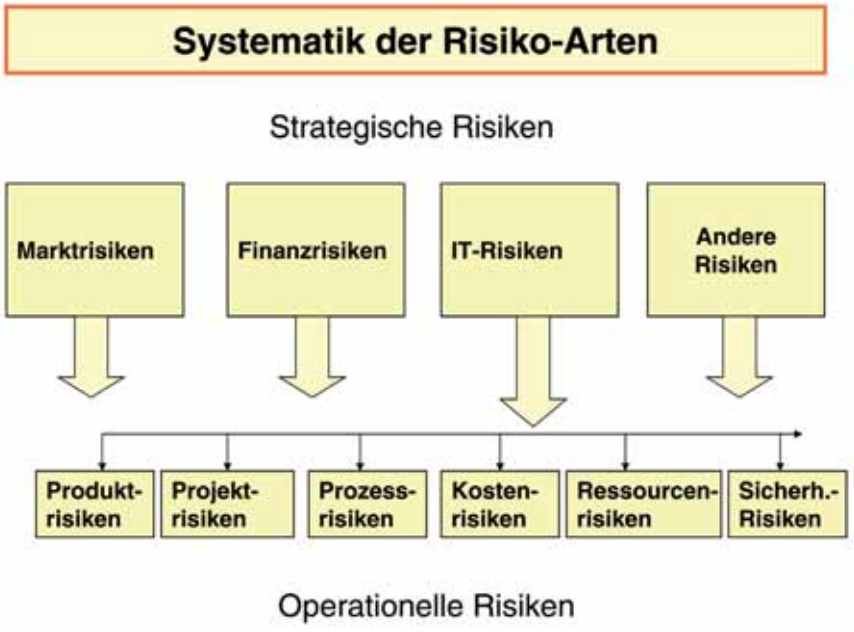
Maßgeschneiderte Suchaufträge + nur 14 Euro* im Monat (* exkl. MwSt., Basis Fair Use)

IT-Risikomanagement:

Aktuelle Herausforderungen, Instrumente, organisatorische Lösungen

IT-Produkte, IT-Prozesse und IT-Projekte sind aufgrund der hohen Komplexität sowie der zu beachtenden zahlreichen Einflussfaktoren nicht frei von Risiken und so großen Unsicherheiten unterworfen.

Ernst Tiemeyer



Arten von IT-Risiken

Sie bergen - das steht außer Zweifel für die Praxis - vielmehr erhebliche Gefahrenpotenziale in sich:

- Menschliches Versagen, etwa durch unzureichende Qualifizierung oder fehlende Leistungsbereitschaft (unqualifizierte bzw. unmotivierte Mitarbeiter).
- Ausfälle von IT-Systemen (etwa von IT-Infrastrukturen oder Softwarelösungen) verursachen immense Zusatzkosten. Sie haben zur Folge, dass vereinbarte Leistungen nicht oder nicht rechtzeitig erbracht werden.
- Fehlende Kontrollen, die den Anreiz auf betrügerisches Handeln erhöhen, können hohen Schaden verursachen.
- Fehlerhafte Abstimmungen und Fehler verursachende Kommunikationsprozesse können die Qualität der IT-Produkte signifikant verschlechtern.
- Eine Vielzahl von Einflussfaktoren kann dazu führen, dass das Erreichen der mit den IT-Projekten, den IT-Produkten sowie den IT-Services angestrebten Ziele gefährdet wird oder gar erhebliche negative Folgewirkungen (etwa aus Fehlern oder Verzögerungen in der Ausführung der IT-Prozesse oder der IT-Projekte) denkbar sind.

Für die Handhabung von IT-Risiken sind inzwischen einige hilfreiche und für die Praxis unverzichtbare Lösungsansätze entwickelt worden, die erhebliche Potenziale zur Zukunftssicherung eröffnen können. Sie helfen unter anderem, IT-Risiken frühzeitig zu erkennen und so zu verhindern, dass IT-Probleme die Geschäftsabläufe beeinträchtigen. Sicherheitslücken können so erfolgreich beseitigt und Haftungsrisiken minimiert werden. In jedem Fall müssen sich die IT-Verantwortlichen vergegenwärtigen,

- welche IT-Risiken bei den IT-Produkten, IT-Prozessen und IT-Projekten zu beachten sind,
- welche Aktivitäten für das IT-Risikomanagement üblich sind und sich bewährt haben (Best Practices),

> *„Ich kann mir nichts vorstellen, was dieses Schiff zum Sinken bringt. Ich kann mir keine Katastrophe vorstellen, die diesem Schiff zustoßen könnte."*
>
> *Kapitän der Titanic, 1912*

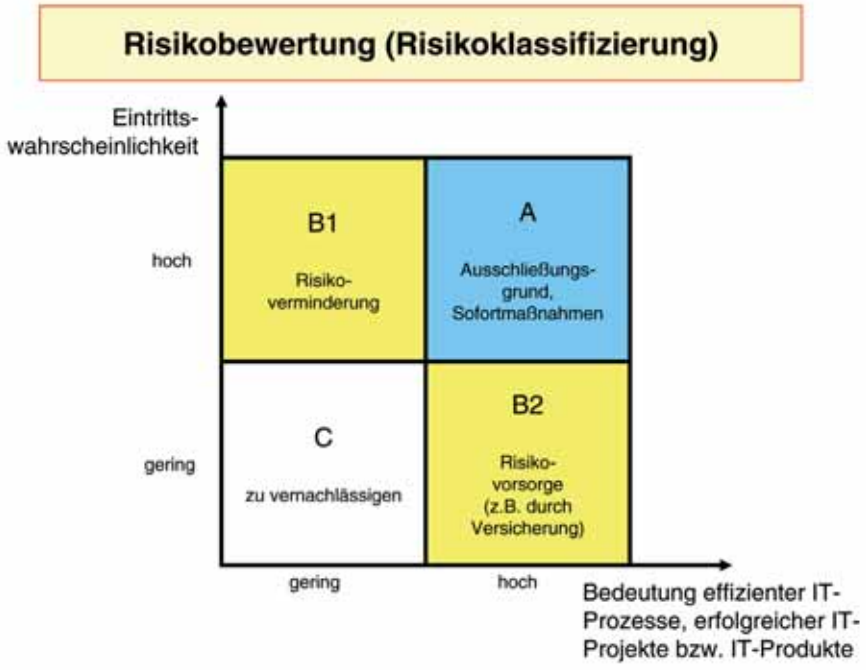
- wie eine Einordnung dieser Aktivitäten aus operativer und strategischer Sicht erfolgen kann sowie
- welche Zielgruppen für IT-Risikomanagement unterschieden werden können.

Zwar sind in größeren Organisationen schon zahlreiche Aktivitäten für eine Professionalisierung im IT-Risikomanagement vorgenommen worden. Die Mehrheit der Unternehmen steht heute aber genau vor der Herausforderung, ein Risikomanagement-System für den IT-Bereich neu aufzusetzen oder grundlegend zu erweitern. Zur Konzeptentwicklung sowie der Optimierung der **Prozesse und Werkzeuge des IT-Risiko-Managements** sind in jedem Fall vier Schritte permanent zu durchlaufen:

- **Risiko-Identifikation:** In einem ersten Schritt sind die IT-Risiken zu identifizieren. Dies geschieht etwa durch Meldungen der beteiligten und betroffenen Personen eines IT-Prozesses, durch die Nutzer der IT-Produkte oder durch die Mitglieder der IT-Projektteams.
- **Risiko-Analyse:** Die identifizierten IT-Risiken müssen anschließend hinsichtlich der Erreichung der Zielsetzungen einer genauen Analyse unterzogen werden. Dabei bietet sich fast immer Teamarbeit an.
- **Risiko-Bewertung:** Risikomelder müssen (ggf. ebenfalls in Abstimmung mit dem Team) einschätzen, mit welcher Wahrscheinlichkeit das Risiko eintritt. Dann wird ermittelt, welches Ausmaß das Risiko in Bezug auf Qualität, Zeit und Ressourcen hat. Festzulegen ist eine Risikokennzahl mit Bezug auf Eintrittswahrscheinlichkeit und Risikoausmaß.

■ **Maßnahmen zur Risikobehandlung:** Es gilt Maßnahmen einzuleiten, die den identifizierten IT-Risiken entgegenwirken, insbesondere natürlich den Risiken, die mit hoher Wahrscheinlichkeit eintreten bzw. wo ein relativ hoher Schaden die Folge sein kann. Bei IT-Prozessen zählt dazu beispielsweise die Anpassung von Zielen, Plänen oder Ressourcen. Ist dieses Potenzial ausgeschöpft, können Risiken auch auf Dritte verlagert werden, etwa durch Outsourcing oder die Vereinbarung von Schadensersatz bei Nichterfüllung von Dienstleistungen durch Dritte.

Eine erste **Feststellung und Konsequenz:** Jeder IT-Verantwortliche ist heute gefordert, potenzielle IT-Risiken frühzeitig zu erkennen und - sofern notwendig - geeignete Gegenmaßnahmen rechtzeitig einzuleiten. In vielen Fällen bietet sich sogar die Position eines speziellen IT-Risikoexperten an (IT-Risk-Manager). Die Umsetzung von IT-Risikomanagement muss sich dabei über mehrere Unternehmensbereiche erstrecken und sämtliche IT-Prozesse, IT-Projekte und IT-Produkte umfassen.



Durch die Risikokategorisierung im Portfolio-Diagramm kann den identifizierten Risiken eine Struktur gegeben werden, die hilft, besonders riskante Bereiche des Prozesses herauszufiltern und sinnvolle Maßnahmen abzuleiten. (Zur Interpretation der Darstellung: A = Ausschließungsgrund, Sofortmaßnahmen erforderlich; B1 = Risikobegegnung durch Verminderung, Gestaltung; B2 = Risikoüberwälzung durch Versicherung; C = vernachlässigen)

Erste Schritte

Erste Schritte im Risikomanagementprozess stellen **systematische Bestandsaufnahmen** zu den Risiken dar, die im IT-Bereich gegeben sind. Insbesondere sollten die IT-Risiken identifiziert werden, die den Bestand des Unternehmens in besonderer Weise gefährden können. Nur durch eine geeignete Systematisierung und Kategorienbildung ist eine differenzierte Risikoanalyse möglich und lassen sich geeignete Maßnahmenbündel ableiten.

Bezogen auf das IT-Management sind folgende **Ansatzpunkte zur Gliederung der IT-Risiken (= Risikokategorien)** denkbar (siehe auch Abbildung der IT-Risikoarten):

- IT-Produkte (Zielerreichung, Qualität der Produkte),
- IT-Projekte (Qualität, Wert für die Stakeholder, Kundenzufriedenheit),
- IT-Prozesse (unter Beachtung von Terminen, Kosten oder Qualität),
- eingesetzte Ressourcen (Personen, Software, Sachmittel etc.),
- IT-Organisation und IT-Security.

Es empfiehlt sich, als Ergebnis der Identifizierung und Systematisierung der IT-Risiken ein **Risikoregister** (Risk Register) zu erstellen, das folgende Bestandteile enthält:

- eine Liste der identifizierten Risiken (List of Identified risks),
- eine Übersicht über die Grundursachen von identifizierten Risiken (Root Causes),
- eine Festlegung zu den Auslösern (Trigger) der identifizierten Risiken (= Risikosymptome oder Warnsignale).

IT-Risiken analysieren und bewerten

Sofern eine Risikoidentifikation vorgenommen wurde, kann in einem nächsten Schritt die Analyse und Bewertung der Risiken erfolgen. Dabei ist sowohl die Eintrittswahrscheinlichkeit als auch die Schadenshöhe eines Gefährdungspotenzials zu bewerten. Ergänzend müssen die Wirkungszusammenhänge der Risiken in Betracht gezogen werden.

Im Rahmen einer **Risikoanalyse** geht es im Kern um folgende **Zielsetzungen** und **Teilaktivitäten:**

- **Bestimmung der Wahrscheinlichkeit,** mit der die Ziele erreicht werden können bzw. Festlegung realistischer Ziele.

Beachten Sie: Beschließt ein Unternehmen bzw. die IT-Leitung, Konzepte und Instrumente des Risikomanagement für den IT-Bereich einzuführen bzw. stärker zu implementieren, empfiehlt es sich, eine Reihe von erfolgsbestimmenden Faktoren besonders zu berücksichtigen:

- Management-Commitment,
- personale Qualifizierung verschiedener Akteure im IT-Risikomanagement,
- Beteiligung verschiedener Personen sowie
- die Einbettung in die Unternehmenskultur.

- **Bewertung von Auswirkungen** zu den identifizierten IT-Risiken.
- **Priorisierung der Risiken und Darstellung dieser Rangordnung** durch Adjektive oder Farben (hoch, mittel, gering; rot, gelb, grün u. s. w.). Es gilt, herauszufinden, welche Risiken die größte Aufmerksamkeit brauchen, indem ihr Beitrag zum Gesamtrisiko in den Prozessen erhoben wird.

Mögliche Auswertungslisten für eine Gruppierung sind:

- Liste der Risiken, die schnell bewältigt werden müssen.

- Liste mit Risiken für zusätzliche Analysen.
- Überwachungslisten für Risiken mit niedriger Priorität.
- Trends in den Ergebnissen der qualitativen Risikoanalyse.

Wichtig ist auch die Einstufung der Dringlichkeit von Risiken. Die zeitkritischen Risiken bzw. Bewältigungsmaßnahmen werden dabei in den Prioritäten nach vorne gereiht. Methodisch beliebt ist hier die Interviewtechnik. Sie kann erfolgen mit Fachleuten, erfahrenen Beteiligten und Stakeholdern, um die Risiken in Wahrscheinlichkeit und Auswirkung zu quantifizieren.

Management von IT-Risiken

Sinn und Zweck eines effektiven IT-Risikomanagements ist nicht nur die Identifizierung von Risiken, sondern vielmehr die Ermittlung von Maßnahmen, um die Risiken von vornherein zu vermeiden bzw. um die zu erwartenden Schäden für die Unternehmung und ihre Kunden möglichst gering zu halten. Dies beinhaltet neben der Identifizierung und Bewertung der Risiken auch die Planung und konsequente Umsetzung von Risikomaßnahmen mit dem Ziel, den IT-Bereich in optimierter Form erfolgreich zu hoher Ergebnisqualität zu führen.

Durch eine Risikosteuerung sollen einzelne IT-Risiken mittels gezielter Maßnahmen dahingehend beeinflusst werden, dass eine Verringerung der Eintrittswahrscheinlichkeit und/oder Begrenzung der Auswirkungen erreicht wird. **Gegenstrategien** können dabei in der Regel eine der folgenden vier Optionen betreffen:

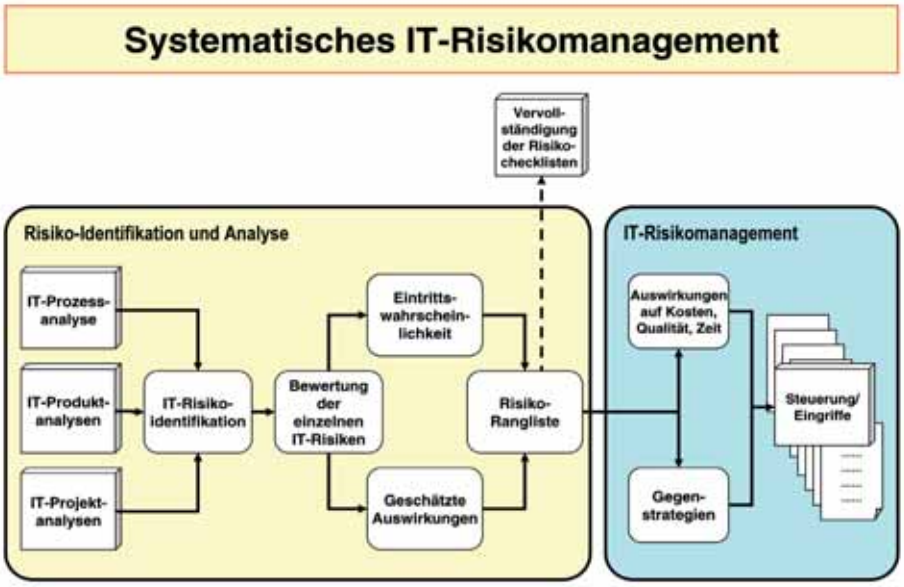
Risikoakzeptanz: IT-Risiken, deren Schadensausmaß und Eintrittswahrscheinlichkeit gering sind, können akzeptiert werden. Diese Risiken werden im Rahmen des IT-Risikomanagements beobachtet, um auf Veränderungen reagieren zu können.

Vermeidung (Avoidance): Mit dieser Strategie versucht man, durch die Änderung der IT-Prozesse bzw. der eingesetzten IT-Produkte und IT-Ressourcen das Risiko überhaupt auszuschließen, z. B. die mit dem Risiko behafteten Aktivitäten/Personen durch andere Aktivitäten/Personen ohne Risiko zu ersetzen. Ein weiteres Beispiel ist die Verwendung bekannter IT-Technologien statt neuartiger Verfahren (Never change a running IT-system). So kann die Eintrittswahrscheinlichkeit eines Risikos gegen bzw. auf Null gebracht werden.

Risko-Übertragung (Transference): Identifizierte IT-Risiken werden in diesem Fall durch Abschluss einer entsprechenden Versicherung oder durch ein Kompensationsgeschäft abgewälzt oder ausgeglichen. Damit wird allerdings das jeweilige IT-Risiko selbst nicht beseitigt. Vielmehr werden die Folgen des Risikos und somit die Verantwortung für die Risikobewältigung an einen Dritten übertragen.

Minderung (Mitigation): In erster Linie wird hier durch geeignete Gegenmaßnahmen versucht, die Eintrittswahrscheinlichkeit des jeweiligen IT-Risikos auf ein akzeptables Maß zu reduzieren, z. B. durch Prozessanpassungen, mehr Ressourcen und ähnliche Optionen. Als Prinzip gilt: Wenn die Eintrittswahrscheinlichkeit nicht gemindert werden kann, muss man versuchen, die Auswirkungen zu reduzieren.

Bevorzugte **Methoden zur Erhebung der IT-Risiken** sind moderierte Workshops, in denen Brainstorming oder strukturierte Befragungstechniken zum Einsatz kommen. Des Weiteren ist die Delphi-Methode als Instrument zur Einbeziehung von Experten gut geeignet. Ergebnisse sind derzeit vor allem die Risikoinventur und die Ereignisanalyse. Die genannten Ansätze weisen im Detail unterschiedliche Stärken und Schwächen auf, wonach entsprechende Einsatzentscheidungen getroffen werden können.



Elemente des IT-Risikomanagement

Dipl.-Hdl.-Ing. **Ernst Tiemeyer**, bekannt durch zahlreiche Buchveröffentlichungen, ist seit mehr als 20 Jahren in leitenden Projektfunktionen sowie als IT-Consultant und im Managementtraining tätig. Schwerpunktmäßig befasst er sich in der Praxis aktuell mit IT-Strategieentwicklung, IT-Projektmanagement, IT-Controlling, IT-Servicemanagement sowie prozessorientierten IT-Anwendungen (GPO, GPM, E-Business-Lösungen).

Fazit

Die Abhängigkeit der Unternehmen und Verwaltungen von einer funktionierenden IT wird immer größer. Hinzu kommt, dass der Wert der installierten IT-Systeme mittlerweile ebenfalls immens ist. Gleichzeitig bietet die IT infolge der verbreiteten Vernetzung und der hohen Komplexität der Systeme zahlreiche Angriffsflächen, die zu einem mehr oder weniger langen Systemausfall mit erheblichen negativen Folgewirkungen führen können. All die aufgezeigten Phänomene verdeutlichen in beeindruckender Weise die Notwendigkeit, ein effizientes IT-Risikomanagement in der Praxis zu etablieren. ❑

Your potential. Our passion.™
Microsoft®

Piraten abwehren. Leicht.

1. Denken Sie wie ein Pirat.
Um einen Piraten zu besiegen, sollten Sie selbst einer sein. Setzen Sie sich einen Papagei auf die Schulter, schnallen Sie sich ein Holzbein um und üben Sie Ihr grimmiges „Harrr Harrr Harrr", das sollte reichen.

2. Drohen Sie ihnen, aber richtig.
Weder die Polizei noch die gerissensten Anwälte lehren einen echten Seebären das Fürchten. Drohen Sie lieber damit, ihm den Rum wegzunehmen, wenn er nicht brav ist.

3. Die Planke!
Drohen Sie mit der Planke, auch wenn es in Ihrem Büro keine (echten) Haie oder Riesenkraken gibt, welche die Piraten verspeisen würden. Mit etwas Glück reicht die bloße Drohung, um den Piraten das Fürchten zu lehren.

4. Entfesseln Sie Ihre Take-One-Bart-Künste.
Schnappen Sie sich den Bart des Schurken und machen Sie eine dekorative Schleife hinein. Seine Freunde werden ihn auslachen und sich dabei zu Tode – effektiv.

Würmer abwehren. Leichter.

1. Implementieren Sie Microsoft Forefront.
Forefront™ macht es Ihnen leichter als jemals zuvor, Ihre Systeme zu schützen. Mit der bedienungsfreundlichen Familie von modernen Client-, Server- und Netzwerk- Sicherheitsprodukten sind Sie Viren und Spyware immer einen Schritt voraus. Fallstudien, Downloads und Neuigkeiten dazu finden Sie auf **easyeasier.at**

Microsoft®
Forefront™

„Schützen Sie Ihren PC mit den neuen Sicherheitsfunktionen von Windows Vista“

Gerhard Goeschl, Sicherheitssprecher, Microsoft Österreich, beantwortet Security-Fragen rund um Windows Vista, Nachfolge-Betriebssystem von Windows XP.

Wo liegt der große prinzipielle Unterschied bei der Sicherheit von Windows XP und Windows Vista?

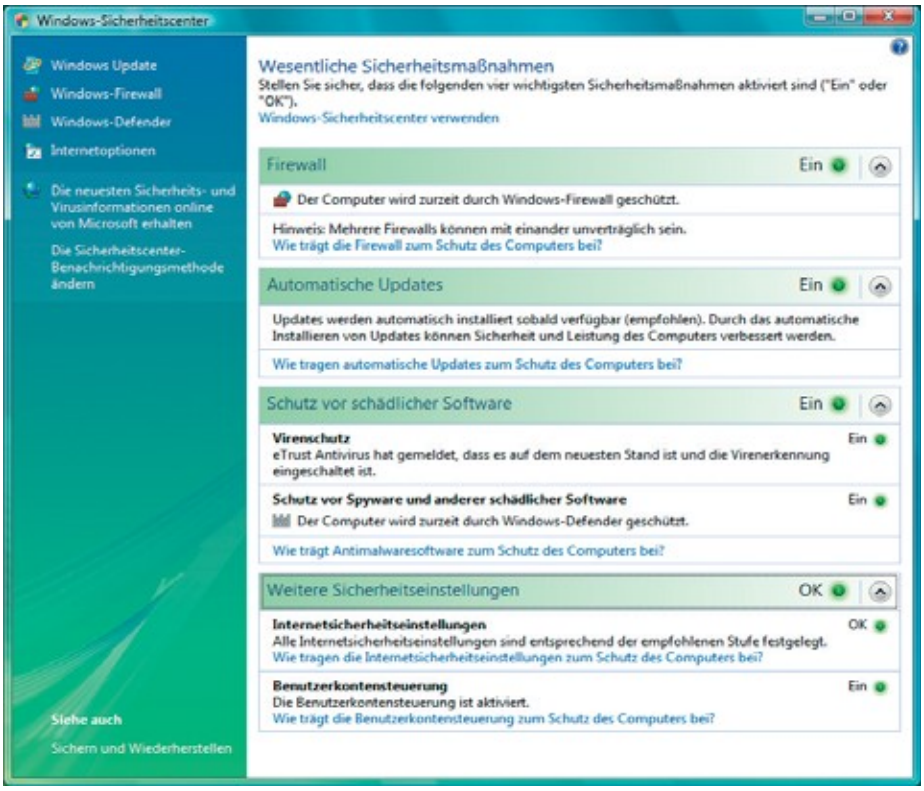
Vor einigen Jahren rief Microsoft-Vorstandsvorsitzender (und damals Chief Software Architect) Bill Gates seine Mitarbeiter auf, die vertrauenswürdige Datenverarbeitung („Trustworthy Computing“) zur obersten Priorität des Unternehmens zu machen. Diese Ankündigung brachte eine Reihe von Änderungen in der Art und Weise mit sich, in der Microsoft Software entwickelt.

In welcher Art kann man Software anders entwickeln? Was genau hat sich da geändert?

Windows Vista ist das erste Betriebssystem, das vollständig gemäß den Richtlinien des Sicherheitsentwicklungszyklus (Security Development Lifecycle, SDL) entwickelt wurde. Der SDL ist ein sicherheitsorientierter Entwicklungsprozess, mit dem die Sicherheit in den Mittelpunkt der Softwareentwicklung gerückt wird. Alle im breiten Rahmen bereitgestellten Microsoft-Produkte müssen diese Richtlinien befolgen. Wer sich hier detailliert einlesen will: Weitere Informationen zu SDL findet man im Buch „The Security Development Lifecycle“ von Michael Howard und Steve Lipner.

Das heißt, der große Unterschied bei der Sicherheit von Windows XP und Windows Vista ist die Programmierung laut dem Sicherheitsentwicklungszyklus?

Durch den SDL ist Windows Vista von Grund auf sicherer, und bietet eine zuverlässigere grundlegende Architektur. Darüber hinaus umfasst Windows Vista zudem neue oder aktualisierte integrierte Sicherheitstechnologien. Diese arbeiten aktiv daran, Sicherheitsbedrohungen zu erkennen und zu verhindern. Alle diese Änderungen bedeuten, dass es sich bei Windows Vista um die bisher sicherste Version von Windows handelt.



Verwalten der Sicherheitseinstellungen an einer zentralen Stelle

Was sind denn die großen Verbesserungen bei Vista zum Thema IT-Sicherheit?

Kurz zusammengefasst: sind es drei Punkte, die den Benutzer am offensichtlichsten schützen:

- das Windows-Sicherheitscenter
- die neue Benutzerkontensteuerung
- der integrierte Windows Defender

Wo kann der Benutzer auf die diversen Sicherheits-Einstellungen zugreifen?

Wenn Sie in Windows Vista die Systemsteuerung öffnen, werden Sie feststellen, dass diese in zehn Funktionalitätsbereiche unterteilt ist. Die meisten sicherheitsorientierten Applets befinden sich in den Kategorien „Sicherheit“, „Programme“ und „Netzwerk und Internet“.

Mit Hilfe des Applets „Sicherheit“ können Sie auf viele der neuen Sicherheitstechnologien zugreifen, die Ihnen unter Windows Vista Schutz bieten (eine genaue Auflistung findet sich in nebenstehender Tabelle). Darüber hinaus lässt sich dort auch nach Windows-Updates suchen, die BitLocker-Laufwerkverschlüsselung aktivieren, Cookies oder den Verlauf löschen und ein Kennwort festlegen, nach dem gefragt werden soll, wenn der Computer aus dem Ruhestand reaktiviert wird.

Über das Applet „Sicherheit“ kann zudem auf einfache Weise auf das Sicherheitscenter zugegriffen werden. Das ist eine zentrale Stelle, von der aus man den Status der Sicherheitseinstellungen und die integrierten Schutzfunktionen des Computers verwalten und überwachen kann.

Wie kann das Windows-Sicherheitscenter den Benutzer besser schützen?

Vor der Einführung des Sicherheitscenters in Windows XP Service Pack 2 (SP2) war die Handhabung der verschiedenen Windows-Sicherheitseinstellungen schwierig. Doch jetzt

Funktion	Beschreibung
Sicherheitscenter	Nach Updates suchen, Sicherheitsstatus überprüfen, automatische Updates aktivieren, Firewallstatus überprüfen, Kennwort bei Reaktivierung des Systems abfragen.
Windows-Firewall	Windows-Firewall ein- oder ausschalten, Programm durch die Windows-Firewall lassen
Windows-Update	Automatische Updates aktivieren, nach Updates suchen; installierte Updates anzeigen.
Windows Defender	Auf Spyware und andere eventuell unerwünschte Software überprüfen.
Internetoptionen	Sicherheitseinstellungen ändern, Cookies löschen, Verlauf löschen.
Jugendschutz	Jugendschutz für beliebige Benutzer einrichten, Aktivitätsberichte anzeigen.
BitLocker-Laufwerkverschlüsselung	BitLocker-Laufwerkverschlüsselung aktivieren.

Tabelle: Sicherheitstechnologien in Windows Vista

benötigt man lediglich das Sicherheitscenter, um sämtliche wichtigen Windows-Sicherheitseinstellungen an einem zentralen Ort zu verwalten. In Windows Vista ist es um einige Funktionen erweitert worden, und damit sogar noch nützlicher.

Das Windows-Sicherheitscenter wird im Hintergrund ausgeführt und sorgt für die aktive Überwachung von vier Funktionalitätskategorien (siehe Abbildung). Firewall, automatische Updates, Schutz vor schädlicher Software (Viren und Spyware) sowie weitere Sicherheitseinstellungen (Einstellungen für Internet und Benutzerkontensteuerung).

Was genau kann der Benutzer dem Windows Sicherheitscenter an Informationen entnehmen?

Mit dem Windows-Sicherheitscenter kann man feststellen, welche Anwendung als Firewall oder als Antivirus- und Antispywarelösung des Computers fungiert. Darüber hinaus kann man den Status der Einstellungen für Firewall, automatische Updates und Benutzerkontensteuerung überprüfen. Das Windows-Sicherheitscenter ist insofern einzigartig, als neben integrierten Windows-Technologien auch der Status von Anwendungen anderer Anbieter überwacht wird.

Welche Einstellungen werden durch das Windows-Sicherheitscenter überwacht?

Durch das Windows-Sicherheitscenter werden die folgenden Einstellungen überprüft:

- Firewall: Ob eine Firewall installiert und ob sie aktiviert ist
- Antivirenprogramm:
  Ob ein solches installiert ist
  Ob die entsprechenden Definitionen auf dem neuesten Stand sind
  Ob die Echtzeitprüfung aktiviert ist
- Antispyware-Software:
  Ob eine solche installiert ist
  Ob die entsprechenden Definitionen auf dem neuesten Stand sind
  Ob die Echtzeitprüfung aktiviert ist

Kann man auch Sicherheitsprogramme von anderen Anbietern in Windows Vista einbinden?

Ja, natürlich kann man auch Sicherheitsprogramme von anderen Anbietern in Windows Vista einbinden. Zur Erkennung der Antiviren- und Firewallprogramme anderer Anbieter verwendet das Windows-Sicherheitscenter zwei Ansätze. Im manuellen Modus wird nach Registrierungsschlüsseln und Dateien gesucht, anhand derer das Windows-Sicherheitscenter den Status der Software ermitteln kann.

Zudem werden WMI-Anbieter (Windows Management Instrumentation) abgefragt, die von den jeweiligen Anbietern bereitgestellt wurden und die den Status der Funktionen zurückgeben. Das bedeutet, dass man Antiviren-, Antispyware- und Firewalllösungen anderer Anbieter einsetzen und seinen Computer dennoch mit dem Windows-Sicherheitscenter überwachen und schützen kann.

Kann das Windows-Sicherheitscenter eigentlich auch zentral verwaltet werden?

Das Windows-Sicherheitscenter kann mit Hilfe von Gruppenrichtlinien gesteuert werden. In Domänenumgebungen ist es daher auch standardmäßig deaktiviert. Man kann es aber trotzdem ganz bewusst wieder einschalten. Um das Windows-Sicherheitscenter zu aktivieren, öffnen Sie den Knoten „Computerkonfiguration\Administrative Vorlagen\Windows-Komponenten\Sicherheitscenter". Der Name der zum Aktivieren benötigten Richtlinie lautet „Sicherheitscenter aktivieren (nur Domänencomputer)".

Wo kann man weitere Informationen zum Thema Sicherheit in Vista bekommen?

Es gibt verschiedene Möglichkeiten zum Thema Sicherheit informiert zu werden. Angefangen über unser Sicherheitsportal, über Newsletter zum Thema Sicherheit bis hin zu diversen Veranstaltungen. Schauen Sie sich zum Beispiel einfach einmal das Video „7 Schritte zu mehr PC-Sicherheit" auf unserem Sicherheits-Portal für Unternehmen an. Oder machen Sie den „Sicherheits-Check für ihr Unternehmen". Sie werden sehen, das ist immer wieder auch etwas Neues dabei. ❑
www.microsoft.com/austria

Ihre Fragen, Kommentare und Anregungen zu diesem Thema richten Sie bitte an:
Gerhard Goeschl,
Sicherheitssprecher
Microsoft Österreich
E-Mail:
GerhardG@Microsoft.com
Telefon: +43 (01) 61 064 460
www.microsoft.com/austria/sicherheit

Weiterführende Links

Sicherheit und Datenschutz in Windows Vista: http://go.microsoft.com/?linkid=5134175
Blog zum Thema Vista: www.VistaBlog.at
Microsoft Sicherheits-Portal: www.microsoft.com/austria/Sicherheit
Sicherheits-Portal für kleine und mittlere Unternehmen: http://www.microsoft.com/austria/kmu/businessthemen/it-sicherheit/sicherheit/default.mspx
Security Guidance Center: http://www.microsoft.com/austria/security/it
Technet Portal: www.microsoft.com/austria/technet

Sicheres Exchange Publishing

ITdesign implementiert redundantes, sicheres Exchange Publishing bei der Grazer Wechselseitigen Versicherung

Die Grazer Wechselseitige Versicherung setzt auf den Microsoft ISA Server 2006 in der Enterprise Edition

Die Grazer Wechselseitige hatte die Anforderung, Mitarbeitern über eine zusätzliche Sicherheitsstufe das Arbeiten mit Exchange auch außerhalb der Firma zu ermöglichen. Dabei wurde großer Wert auf eine ausfallssichere Konzeptionierung gelegt. Den Mitarbeitern sollten die Dienste ActiveSync, Outlook Web Access und Outlook RPC/HTTPS zur Verfügung stehen.

ITdesign wählte als Produkt den Microsoft ISA Server 2006 in der Enterprise Edition. Dieses Produkt von Microsoft zeichnet unter anderem eine sehr gute Cluster-Funktion, hervorragende Sicherheitsmerkmale und eine perfekte Integration in die bestehende EDV-Landschaft aus.

Ausfallsicherheit und Loadbalancing

Der ISA-Server-2006-Cluster bietet neben der Ausfallssicherheit auch ein Loadbalancing. Zu einem späteren Zeitpunkt werden diese beiden Server auch in getrennten Serverräumen ihren Dienst verrichten.

Da sämtliche HTTPS-Requests auf den ISA-Servern terminiert werden, kann dieser mittels integrierten Filtern den Netzwerkverkehr scannen und auf allfällige, ungültige Packete scannen. Durch diese Application-Layer-Gateway-Funktion ist es nicht möglich, Pakete, die nicht zu der jeweiligen gepublishten Funktion gehören, einzuschleusen.

Da der ISA-Server den HTTPS Traffic in HTTP umwandelt, können - wenn gewünscht - in einer zweiten Sicherheitsstufe die HTTP-Pakete nochmals auf ihre Gültigkeit geprüft werden.

Der Microsoft ISA Server 2006 bietet neben oben beschriebenen Exchange-Publishing Funktionen noch eine Vielzahl an zusätzlichen Features.

Herauszustreichen ist wohl die die Application-Layer-Gateway-Funktion für SMTP und WEB, DNS, LDAP, FTP, POP3, u. v. a. m. Einige dieser Filter, die nicht wie herkömmliche Firewalls auf Portebene, sondern auf Paketebene den Netzwerkverkehr inspizieren sind auch auf die eigenen Bedürfnisse anpassbar.

Weitere Funktionen:

- Secure Publishing von SharePoint Portal Server und WEB Server im allgemeinen,
- Proxy Server für Clients,
- RAS/VPN Endpoint für Clients mit Quarantänefunktion,
- VPN Server to Server,
- Authentication über Kerberos,
- LDAP, Zertifikate,
- ein Intrusion Detection und DNS Attack Detection System ...

Für einen detaillierten Überblick über alle Funktionen findet sich auf der Website www.microsoft.com/isaserver ein guter Einstiegspunkt.

Fazit

Für die Grazer Wechselseitige stellen diese vielfältigen Einsatzmöglichkeiten eine gute Investition in die Zukunft dar, da mit dem Microsoft ISA Server 2006 sehr flexibel auf Anforderungen von allen Seiten reagiert werden kann.

Für weitere Informationen steht Ihnen Herr Robert Milberger gerne zur Verfügung.

robert.milberger@itdesign.at
www.itdesign.at

Grazer Wechselseitige Versicherung

„Verlässlicher Versicherungsschutz für alle“ war das Motto Erzherzog Johanns, als er im Jahre 1828 die Grazer Wechselseitige gründete. Seit damals hat sich aus der ursprünglichen Feuerversicherung ein vielseitiges Unternehmen entwickelt. Heute handelt es sich um den fünftgrößten Versicherungskonzern Österreichs mit der Konzernzentrale in Graz. Die jährlichen Prämieneinnahmen betragen rund 402 Mio. Euro, die Anzahl der verwalteten Versicherungsverträge beträgt über 1,6 Mio. Das Unternehmen besitzt Direktionen in allen Landeshauptstädten, rund 100 Bezirksbüros und über 1.200 Mitarbeiter. Dazu kommen Versicherungs-Tochtergesellschaften in Slowenien, Kroatien, Ungarn, Serbien, Bosnien-Herzegovina, Ukraine, Bulgarien, Rumänien und Moldavien. www.grawe.at

Oscarreife IT-Security-Lösung in den Constantin Kinos

Microsoft Forefront für Exchange sorgt für ungetrübtes Kinovergnügen

Vorne in den Sälen die freundlichen Mitarbeiter, hinter den Kulissen eine mit innovativer Akribie arbeitende IT: in den Kinos der Constantin-Gruppe erwarten Kinogänger oscarwürdige Leistungen, an sieben Tagen der Woche. Gemeinsam mit dem heimischen IT-Vorreiter mii ag wurde ein undurchlässiger Sperrwall gegen Bedrohungen aus dem Internet errichtet, der trotz höchster Sicherheit komfortables Arbeiten ermöglicht.

Langsam gehen im bis auf den letzten Platz gefüllten Kinosaal die Lichter aus. Ein Blockbuster hat Premiere. Die lebhaften Gespräche verstummen. Endlich ist es soweit! Doch während es sich die Zuseher ahnungslos gemütlich machen, läuft dem Filmvorführer eiskalter Schweiß über den Rücken: Die Vorführung fällt aus.

Ein Alptraum, der in den Filmtheatern der Gruppe niemals Wirklichkeit werden darf. Denn Constantin setzt mit mittlerweile 30 Spielstätten, zu denen 19 Cineplexx-Großkinos und elf kleinere Kinos zählen, den Standard für gehobenes Freizeitvergnügen. Mehr als 7 Mio. Filmfreunde zieht das hochwertige Angebot jährlich an. Ihnen fühlt sich das Unternehmen verpflichtet.

Keine Vorführung ohne IT

Dafür, dass ein Kinoheld pünktlich zur angekündigten Zeit auf der Leinwand erscheint, trägt im digitalen Zeitalter vorrangig die engagierte und innovative IT-Crew Sorge. Denn in jenen Kinos, die bereits auf digitale Technologie umgestellt haben, bringt erst ein spezieller Security Key die Festplatte, die in dem Fall die ehrwürdige Filmrolle abgelöst hat, dazu, sich zu drehen. Diesen Schlüssel erhält jedes Kino von der jeweiligen Verleihfirma kurz vor Filmstart per E-Mail. Wie leicht könnte gerade eine solches Mail einer scharf eingestellten Spamabwehr ins Netz gehen! Dann nähme die Katastrophe ihren Lauf: kein Key, keine Vorstellung.

Doch ein undurchdringlicher Schutz vor Bedrohungen aus dem Internet ist für die Kinogruppe von existenzieller Bedeutung. Denn die Standorte in ganz Österreich werden per Mail mit allen zum Betrieb benötigten Informationen versorgt. „Verständlich, dass wir außerordentlich hohe Ansprüche an Sicherheit stellen - übrigens, nicht nur in Bezug auf E-Mail, sondern bei unserer gesamten Präsenz im Internet und natürlich auch beim Online-Ticketkauf“, macht Michael Redtenbacher, der Constantin-IT-Verantwortliche, die oberste Priorität deutlich. „Gleichzeitig muss gewährleistet sein, dass unsere User ihre Arbeit uneingeschränkt erledigen können. Schließlich gilt gerade für uns: The show must go on!“

Kampf dem Bösen

In höchstem Maß konträre Anforderungen also. Mit der Auflösung solcher Widersprüche wurden die Experten des IT-Dienstleisters mii ag betraut, in den Constantin aus Erfahrung volles Vertrauen setzt.

Im Zuge der IT-Modernisierung wurde zunächst Microsoft ISA 2000 auf 2004 upgedatet. ISA dient als Application Firewall und Reverse Proxy. In der modernen IT-Welt der Constantin-Kinos arbeiten die Benutzer an den verteilten Standorten nur noch mit einem Browser. Der Zugang zu den gemeinsamen Dokumenten erhalten sie über Outlook Web Access (OWA). ISA sorgt beispielsweise dafür, dass wesentliche Informationen über technische Störungen, die ein Kino über das interne Service-Ticketing-System an den Support oder an das Facility Management meldet, ihr Ziel verlässlich erreichen.

The Oscar goes to ...

An exponierter Stelle im Abwehrkampf ist Microsoft Forefront tätig, das das zuvor eingesetzte Sybari Antigen ablöste. Das Sybari-Produkt hatte von Anfang an sowohl durch Sicherheit als auch durch komfortable Handhabung überzeugt. Diese Features blieben auch nach der Eingliederung bei Microsoft erhalten. „Forefront ist leicht zu administrieren“, schildert mii-Projektleiter Christoph Wilfing. „Virensignaturen und Spamfilter werden regelmäßig automatisch upgedatet, die Administratoren sind dadurch in ihrem umfangreichen Aufgabengebiet enorm entlastet. Kompromisslose Sicherheit ist für Constantin unabdingbar“, ist sich Wilfing im Klaren. „Mit seiner nahtlosen Integration im Microsoft Exchange Server 2007 ist Forefront daher genau die richtige Lösung.“

Gäbe es ihn, den Oscar für herausragende Leistungen hinter den Kulissen, die Constantin-IT-Crew, die Microsoft-Experten der mii ag und MS Forefront hätten wohl beste Chancen, damit ausgezeichnet zu werden.

www.mii.at

Small is beautiful: Die kleinsten Firewalls der Welt

Der Wunsch, technische Geräte immer kleiner zu gestalten, ist ein allgemeiner Trend. Die Grenzen werden meistens durch physikalische Limits anderer Art vorgegeben wie menschliche Finger zur Eingabe von Daten oder notwendige Steckplätze z. B. für Netzwerkkabel.

Manfred Wöhrl

Gatekeeper Pico (Bild: Yoggie)

Bei meinen Firewall-Recherchen bin ich auf eine interessante Lösung gestoßen - eine Firewall in Kleinstformat mit zwei Netzwerkschnittstellen (die eine echte Appliance zumindest haben muss). Nur - wie schütze ich meinen Notebook, wenn er per WLAN angebunden ist?

Ganz einfach, die Mini-Firewall von YOGGIE („Gatekeeper Pro") hat auch ein USB-Kabel. Dieses an den Notebook angedockt und ein Treiber installiert und die Firewall schützt auch den Mobile-User durch eine externe Firewall. Dieser NDIS-Treiber „hängt" sich zwischen Rechner und Betriebssystem, fängt alle Anfragen, die per Netzwerk von außen kommen ab, lenkt diese über den USB-Anschluss an die Firewall und prüft die Anfrage. Erst bei erlaubter Aktion wird die Anfrage an das Betriebssystem übergeben.

Um das Ganze noch zu perfektionieren wurde die YOGGIE-Firewall noch einmal verkleinert. Wenn ich auf die „unnötig großen Netzwerkanschlüsse" verzichte - und die gesamte restliche Funktionalität beibehalte, genügt doch eigentlich ein USB-Stecker! Und das wurde mit dem YOGGIE („Gatekeeper Pico") realisiert. Ein USB-Stecker mit vollwertigem LINUX-Firewallsystem.

Wie die meisten modernen Firewallsysteme bietet auch die YOGGIE-Firewall u. a. weitere Dienste an: Anti-Spam, Anti-Phishing, Antispyware, Antivirus, Transparent E-Mail Proxies (POP3, SMTP), Transparent Web Proxies (HTTP, FTP), Intrusion Detection System/Intrusion Prevention System, VPN Client.

Gatekeeper-Pro und Gatekeeper-Pico sind bereits um unter 200 Euro zu bekommen - inklusive Patternupdate der zusätzlichen Schutzsoftware für ein Jahr. Für einen unternehmensweiten Schutz von Notebooks gibt es von YOGGIE auch eine zentral managebare Version mit einem Server in der Zentrale. Die genaue Arbeitsweise einer solchen Lösung würde den Rahmen dieses Artikels sprengen.

www.yoggie.com

Dr. **Manfred Wöhrl** ist Geschäftsführer der R.I.C.S. EDV-GmbH (Research Institute for Computer Science, www.rics.at), spezialisiert auf Securitychecks und Security-Consulting. Dr. Wöhrl ist Vortragender und Betreuer bei einer Reihe von Seminaren und Tagungen und gerichtlich beeideter und zertifizierter Sachverständiger und im Vorstand der ADV und itSMF-Austria.

Wer dieses Produkt im Echtbetrieb sehen will - es wird am 28.11.2007 im Rahmen eines ADV-Seminars mit anderen Sicherheitslösungen für Notebooks praktisch demonstriert.

www.adv.at/veranstaltungen

IT design
software projects & consulting

Anton Freunschlag-Gasse 49
A-1230 Wien
Tel.: +43(1)699 33 99-0
office@itdesign.at
www.itdesign.at

mii

mii - marcus izmir informationsmanagement ag
Lerchenfelder Straße 2/203, 1080 Wien
tel: (+43) (0)1 4070587-0
fax: (+43) (0)1 4070587-77
E-Mail: welcome@mii.at
http://www.mii.at

Datenlöschung - das zweite Standbein der Datensicherheit

Datenlöschung ist ein immer wichtigeres Thema. Ein verantwortlicher Umgang mit Informationen bedeutet nicht nur die Sicherung, sondern auch das endgültige Löschen von Daten, um Zugriff durch Unbefugte zu verhindern.

Unternehmen, die intern Festplatten wiederverwerten und gebrauchte Hardware ausrangieren oder verkaufen wollen, stehen vor der Aufgabe, in großem Maße mit hoher Sicherheit und mit einer entsprechenden Dokumentation Daten zu löschen.

Im Falle der Weiterverwendung sollte man effektiv löschen, ohne die Festplatte zu zerstören. Angesichts der Fülle möglicher Methoden ist Datenlöschung ein weites Feld. Ein Leeren des Papierkorbs oder das Formatieren löscht keine Daten, sondern gibt nur die entsprechenden Sektoren einer Platte zum Neubeschreiben frei. Die Informationen sind jedoch weiter vorhanden. Mit auf dem Markt erhältlicher Datenrettungs-Software gelingt die Wiederherstellung selbst IT-Laien.

Wer wirklich Daten löschen will, muss also mehr tun. Er kann die Daten überschreiben oder physikalisch vernichten.

Die Software Ontrack® Eraser™ löscht firmeninterne und vertrauliche Daten dauerhaft und sicher. So sind zum Beispiel bei der Rückgabe von Leasing-Geräten, einem User-Wechsel oder bei der Weitergabe eines PCs die ursprünglichen Daten vor dem Zugriff Dritter geschützt. Mit diesem Programm lassen sich Daten schnell und effizient durch mehrfaches Überschreiben der Festplatten so löschen, so dass eine Wiederherstellung der Daten unmöglich ist.

Für die physikalische Vernichtung eines Datenträgers bietet Kroll Ontrack den Degausser. Mit dem Degausser können nicht mehr ansprechbare Speichereinheiten sowie austauschbare magnetische Datenträger wie Bänder und ZIP-Laufwerke zuverlässig gelöscht werden.

Der Degausser löscht Datenträger mit Hilfe eines starken Magnetfeldes. Auf diese Weise werden sämtliche Informationen unwiederbringlich zerstört und die Daten können nicht wiederhergestellt werden.

www.krollontrack.at

„Für das Konzept der IT-Sicherheit in Unternehmen ist die sichere Datenlöschung unerlässlich." - **Margret Horn**, Senior Account Manager bei Kroll Ontrack

PROMOTION

Smartcards bei Energie AG

Durch die Einführung eines multifunktionalen Mitarbeiterausweises setzte das Unternehmen ein anspruchsvolles PKI-Projekt in die Tat um, das neben erheblich verbesserter Absicherung der Geschäftsdaten auch wichtige Arbeitserleichterungen für die Anwender mit sich brachte.

(Bild: Energie AG)

Mit den Bereichen Gas, Strom, Wärme, Abfallwirtschaft und Wasser ist die in Linz beheimatete Energie AG einer der großen österreichischen Infrastrukturkonzerne. Als Dienstleister beschäftigt das Unternehmen ca. 900 mobile Notebookanwender, vom Servicetechniker bis zum Vertriebsbeauftragten mit der Anforderung, sich von überall her via Internet ins Firmennetz einwählen zu können. Die ständig wachsende Gefahr des Notebookdiebstahls und somit auch missbräuchlicher Verwendung von teils hochsensiblen Kunden- und anderen Unternehmensdaten ließen bereits 2002 den Entschluss reifen, diese Bedrohungen für die IT-Sicherheit durch eine neue Smartcard auszumerzen.

Ein kontaktloser Mitarbeiterausweis für die Kantine und die Zeiterfassung war zwar schon seit Jahren im Einsatz, wichtige Security-Funktionen wie eine vereinfachte Authentifizierung beim Remotezugang und auf den Workstations oder die Verschlüsselung von Festplatten jedoch fehlten.

Und so informierte sich das Unternehmen in einem Workshop zum Thema PKI und Kryptographie noch im selben Jahr über aktuelle Technologien und Einsatzmöglichkeiten im Haus. Schnell erkannte man Lösungsansätze und beauftragte den IT-Security-Dienstleister Integralis mit der Erstellung einer Vorstudie. Erste Zielsetzung war, den laufenden Betrieb bei der Energie AG näher zu erfassen und auftretende Schwachstellen genau zu dokumentieren. Auf Grundlage des so entstandenen Arbeitspapiers startete die IT-Abteilung in 2004 ein Pilotprojekt mit ca. 20 Teilnehmern.

Schwierigkeiten überwinden

Doch schon in der Planungsphase stieß man auf erste Schwierigkeiten und musste teils neue Lösungswege beschreiten. Bereits in der Vorstudie war vorgesehen, das Projekt auf Basis einer Novell Certification Authority umzusetzen, da das Produkt bereits im Hause war und auch schon als Masterdirectory diente. Im weiteren Verlauf stellte sich jedoch heraus, dass verschiedene Komponenten des Herstellers in den Bereichen PKI und Kryptographie nicht wie gewünscht funktionierten oder zur Verfügung standen. „Im Ergebnis mussten wir umplanen und haben verschiedene Novell-Komponenten, hauptsächlich die Certification Authority, durch Produkte von Microsoft ersetzt“, erklärt Ingenieur Roland Ott von Konzern-IT-Services die damalige Situation.

So wurde zwar die gesamte Benutzerverwaltung wie auch die Netzwerkanmeldung auf Novell belassen, mittels eines Tools von Novell werden die Benutzer nun aber vom Novell Directory NDS ins Microsoft Directory hinein synchronisiert. „Durch diese Probleme haben wir zwar einige Zeit verloren, schließlich konnten wir mit der neuen Lösung den Piloten aber Mitte 2004 erfolgreich abschließen und das Projekt ausschreiben“, zeigt sich der Securityverantwortliche letztlich zufrieden.

Die Vergabe erfolgte dann im Herbst 2004 an den deutschen IT-Dienstleister Integralis als Generalunternehmer. „Integralis war schon seit 1997 als Lösungsanbieter bei uns im Haus und wir waren der Ansicht, dass das Unternehmen mit seinem Partner ActivIdentity das Thema Security am breitesten abdecken konnte“, begründet Ott die damalige Entscheidung.

Im Frühjahr 2005 startete die Energie AG nach Implementierung der Serverinfrastruktur mit dem Rollout. „Wir haben mit dem Rollout bei den leidensfähigen Abteilungen, also bei uns in der IT, begonnen“, so Roland Ott. „Auf diese Weise konnten wir dem Projekt noch den letzten Feinschliff verpassen und Kleinigkeiten bereinigen.“ Aber auch hier verlief nicht alles nach Plan.

So hatten die für das Rollout zuständigen Mitarbeiter ständig mit knappen Ressourcen zu kämpfen, wandelte sich die Energie AG von einem Unternehmen mit 2.000 Angestellten doch binnen weniger Jahre durch zahlreiche Akquisitionen und damit verbundenen Umstrukturierungen bis ins Jahr 2006 zu einem Konzern mit heute 6.000 Mitarbeitern.

Hinzu kam auch, bedingt durch den Neubau des Firmengebäudes am Standort Linz, die Zersplitterung der Zentrale auf drei Ausweichquartiere. Da kam die Möglichkeit, das Rollout des neuen Mitarbeiterausweises dezentral, sozusagen im „Selfservice“, durchzuführen, gerade recht.

Initialisiert wurde die neue Smartcard zentral durch die Personalabteilung. Dies war nötig, da sich auf der neuen Karte nun sowohl der alte bereits für Kantine und Zeiterfassung genutzte Chip als auch der neue befanden. Da beide mit unterschiedlichen Technologien

arbeiten, mussten sie auch unterschiedlich initialisiert werden. So vorbereitet, wurde die neue Karte dann durch einen Vor-Ort-Service mit Unterstützung des zentralen User Helpdesks in den einzelnen Standorten ausgestellt. „Wir mussten auch darauf achten, den Übergang fließend zu gestalten, da die Mitarbeiter ja noch die alten Mitarbeiterausweise besaßen, die Zug um Zug ausgetauscht werden mussten", erklärt der IT-Fachmann das Vorgehen.

Bedingt durch eine Vielzahl von Standorten wie Kraftwerken und Servicezentren in vielen Ländern wäre ein zentrales Ausstellen des Ausweises auch nur schwer möglich gewesen.

Akzeptanz schaffen

„Durch die enge Einbindung der Personalabteilung, der Rechtsabteilung und des Betriebsrates von Beginn an, konnten wir vielen Fragen und Problemen aus dem Weg gehen", erläutert Ott. „So erzielten wir bereits in diesem frühen Projektstadium großes Verständnis hinsichtlich der Verbesserungen für den einzelnen Mitarbeiter. Außerdem gab es ja schon seit Jahren einen Ausweis für Kantine und Zeiterfassung, so dass die Einführung einer neuen Karte die Anwender nicht völlig unvorbereitet traf."

Wichtig war der IT aber auch die Sichtbarkeit des Projektes durch die Geschäftsleitung. „Ohne die Unterstützung der Geschäftsleitung hätten wir nie die nötige Akzeptanz für das Thema bekommen", weiß Ott.

Mehrwerte erzielen

Um aber auch bei den Mitarbeitern eine große Akzeptanz für das Projekt zu erreichen, griff die IT zu einem kleinen Trick. Sie verknüpfte das Smartcard-Projekt mit dem Thema Single-Sign-on. Dies war wichtig, um dem Anwender mit der Einführung einer abstrakten und neuen Technologie einen sofort sichtbaren Mehrwert zu verkaufen.

„Das Thema Single-Sign-on wurde von den Usern von Beginn an sehr positiv aufgenommen, sahen sie hierin doch eine sofortige Verbesserung ihrer Arbeitsabläufe", so Roland Ott. „Bei der Vielzahl der sich bei uns im Haus befindlichen Systeme kann man sich vorstellen, was da an Passwörtern mit all den Problemen und Zeitaufwand durch Verlust, Vergessen oder Diebstahl zusammenkam. Für uns bedeutete der Wegfall nicht nur eine erhebliche Verbesserung der Sicherheit, sondern auch eine signifikante Entlastung unseres User Helpdesks."

Als weiterer großer Vorteil erwies sich der nun abgesicherte Remotezugang für die Notebookanwender. Quasi als kleines Network-Access-Control-Projekt (NAC) am Rande wurden alle voreingestellten und nicht veränderbaren Firmenlaptops mit einem Check Point Secure Client ausgestattet und bei jeder Anmeldung zentral auf die Sicherheitsbestimmungen hin abgeprüft. Zuvor nutzten die mobilen Anwender zur Anmeldung einen Token und hatten so einen umständlichen und eingeschränkten Zugang zum Firmennetz. „Heutzutage sind unsere Notebooks so abgedichtet, dass die Mitarbeiter von jedem Ort mit Internetzugang uneingeschränkten Zutritt zum gesamten Unternehmensnetzwerk haben, eine sehr große Arbeitserleichterung für alle."

Fazit

Zurückblickend zeigt man sich bei der Energie AG mit dem Verlauf des Projektes sehr zufrieden, wenn auch Integrationsprobleme einzelner Produkte und die Umstrukturierungsphase des Konzerns den Zeitplan etwas durcheinander würfelten. Das Ziel, mit der eingeführten Lösung Mehrwerte für Mitarbeiter wie das Unternehmen zu schaffen, sieht Roland Ott klar erreicht.

„Das neue Anmeldeverfahren mit Single-Sign-on, der abgesicherte Remotezugang ins Firmennetz und nicht zuletzt die erweiterten Funktionalitäten des neuen Mitarbeiterausweises wurden von den Anwendern uneingeschränkt angenommen", freut sich Ott über den Erfolg. Mit dem geplanten Rückzug in die dann fertig gestellte Konzernzentrale sollen noch weitere Funktionen wie Gebäude-, Raum- und Tiefgaragenzutrittsmanagement hinzukommen. ❑

www.integralis.at

www.datasystems.at

IT-Kompetenz aus einer Hand.

SOFTWARE | HARDWARE | SERVICES – UNSER KNOW-HOW FÜR IHREN ERFOLG.

Data Systems Austria ist der zentrale Ansprechpartner für alle Fragen rund um die IT. Unsere Spezialisten verfügen über umfassendes Know-how in allen IT-Bereichen – von der ERP-Lösung über Branchensoftware, DMS und CRM, über Hardware und Infrastruktur bis hin zu umfassenden Services. Wir erarbeiten bedürfnisorientierte, individuelle Turnkey-lösungen, die Sie in jedem Bereich optimal unterstützen.

Was zählt, ist der Blick aufs Ganze. Denn wir wollen, dass Ihre Strategien sicher zum Erfolg führen.

DATA SYSTEMS AUSTRIA

DATA SYSTEMS AUSTRIA AG & Co KG · 1234 Wien · Liesinger-Flur-Gasse 2 · T: 01/60504-0 · www.datasystems.at · info@datasystems.at

prokesch · grafik & design

Jenseits von Gut und Böse

Der Perimeter zwischen Innen und Außen - zwischen (vermeintlich) sicher und unsicher - ist im Verschwinden begriffen. Die neuen Herausforderungen: Ein nicht grundlegend neues, aber zunehmend vermischtes Bedrohungsbild steht einer wachsenden Zahl weit verstreuter Benutzer und Endgeräte gegenüber.

Alexander Hackl

Die Security-Roadshow des IT-Marktforschers IDC gilt als Trendbarometer in Sachen IT-Sicherheit

Die jährliche Security Roadshow des IT-Marktforschers IDC gilt als Trendbarometer in Sachen IT-Sicherheit. Rund 150 IT-Verantwortliche aus österreichischen Unternehmen quer durch alle Branchen diskutierten mit Anbietern von IT-Sicherheitslösungen wie Qualys, Phion, Juniper Networks oder Xyzmo Software über Bedrohungen, Strategien und Lösungen. Ein Fazit der heurigen Veranstaltung: Das Thema hat bei IT-Verantwortlichen nach wie vor höchste Priorität. Dazu IDC-Österreich-Geschäftsführer Joachim Seidler: „Der Security-Markt boomt weiterhin. Wir prognostizieren global ein jährliches Wachstum für Security Services von 18,9% für die nächsten fünf Jahre, in Westeuropa steigt der Geschäftsbereich der Managed Security Services jährlich um 21,3% bis 2011."

Aber an der Frage, ob die wachsenden Sicherheitsbudgets auch richtig angelegt werden, scheiden sich die Geister. Macht mehr Security ein Unternehmen automatisch sicherer? Bjarne Kaiser Lauritzen, Europa-Vizepräsident des Netzwerk-Equipment-Anbieters Juniper, beantwortet die Frage im MONITOR-Gespräch schlichtweg mit „Nein".

Ein Grundschutz mit Firewalls, Virenabwehr und Co sei zwar erforderlich, aber den hätten die meisten Firmen ohnehin. „Die größte Gefahr geht von leichtsinnigen Benutzern aus. Nach wie vor sind viele Firmen-PCs mit Passwörtern auf gelben Post-its vollgeklebt. Und nicht selten geben sich Hacker am Telefon als Support-Mitarbeiter aus, erfragen Passwörter und bekommen bereitwillig Auskunft."

Regeln gegen den Leichtsinn

Das althergebrachte Bild, dass das Böse von außen droht, wird so ad absurdum geführt. Und wo will man auch heutzutage die Grenze zwischen innen und außen ziehen? Dazu Lauritzen: „Die Netzwerke haben sich in den letzten zehn Jahren grundlegend verändert. Immer mehr Filialen und eine Flut mobiler Endgeräte sind eingebunden. Netzwerkperimeter können auf der ganzen Welt verteilt sein."

Die Lösung für dieses Problem sieht Lauritzen in einer feingranularen Security Policy, die den Sicherheitsstatus von Benutzer, Standort und Endgerät berücksichtigt. Für die praktische Durchsetzung der Regeln hat Juniper die Unified-Access-Control (UAC)-Lösung im Portfolio. Sie setzt sich aus einer Vielzahl von Elementen zusammen. Der Infranet Controller dient als zentralisierter Policy Manager, während es sich beim UAC-Agent um eine dynamisch downloadbare Endpunkt-Software handelt. Hinzu kommt eine flexible Zusammenstellung von Policy-Enforcement-Punkten, zu denen Juniper Firewalls und/oder beliebige 802.1X-fähige Switches oder Wireless Access Points gehören. Der Kunde hat damit die Möglichkeit zur Realisierung von Zugangskontroll-Konzepten in Campus-, Datencenter- und Zweigstellenumgebungen mit leitungsgebundener oder drahtloser Vernetzung. Auch die Anwendungsebene wird mit einbezogen. „Unser System kontrolliert, welcher Benutzer was von welchem Endpunkt aus macht. Ich persönlich kann zum Beispiel im WLAN des Wiener Flughafens E-Mails lesen, aber nicht verschicken - entsprechend der Juniper-Policy."

Management der Ähnlichkeiten

Auch Phion-CEO Wieland Alge sieht das Verschwinden des Innen/Außen-Perimeters als die eigentlich neue Herausforderung in der Security: „Bei den Bedrohungsszenarien gibt es nichts komplett Neues. Das Bedrohungsbild ist aber ein vermischteres geworden. Wirklich neu für die Unternehmen ist die schiere Masse an Notebooks und mobilen Geräten. Darum liegt jetzt ein stärkerer Fokus auf dem Thema End Point Security. Das ist ein

Paradigmenwechsel, denn dadurch wechseln auch die Verantwortlichkeiten. Der User als Kommunikationsteilnehmer ist quasi ‚Trusted Member'. ‚Innen' ist nicht mehr automatisch gut und außen nicht mehr automatisch böse."

Die technischen Möglichkeiten, Policies für User, Endpoint und Anwendungen unter einen Hut zu bringen, gibt es. „Bei 1.000 Mitarbeitern ist nur wieder ein Management-Problem. In der Security geht es um das Management von ähnlichen Dingen. Im Laufe ihrer Nutzung werden selbst gleiche oder ähnliche Geräte und Systeme immer verschiedener. Man muss die Synergie in der Ähnlichkeit finden, eine Mischung zwischen individuellem Management und Profil." Generell ortet Alge ein reiferes Kaufverhalten der Kunden. „Der Business-Nutzen steht mehr im Vordergrund. Nicht „Best of Breed", sondern „Best of Need" ist jetzt die Devise. Unternehmen kaufen nicht mehr unreflektiert gleich jedes neue Feature. Sie analysieren ihre individuellen Sicherheitsanforderungen und besorgen sich dann das, was sie wirklich brauchen. Und die Analyse, was schützenswert ist, fällt bei unterschiedlichen Firmen und Branchen auch sehr unterschiedlich aus", so Alge.

Suche nach der Achilles-Ferse

Die Telekom Austria überlässt bei der Analyse ihres Schutzbedarfs nichts mehr dem Zufall. Auf der IDC-Konferenz stellte sie ein neues Kleinod ihres Sicherheitsmanagements vor: ein Vulnerability Management System. Für die automatisierten Vulnerability-Scans wird der QualysGuard, eine Plattform für Risk- und Compliance-Management eingesetzt. „Im Risikomanagement bewerten wir sowohl die Verletzlichkeit als auch den Grad der Schutzwürdigkeit von Systemen und Daten. Nicht jede Vulnerability muss sofort beseitigt werden", erklärte TA-Mann Krystof Müller. Beim Telekom-Marktführer ist das Vulnerability-Management in ein ganzes Konvolut an Sicherheitsframeworks eingebettet.

In der Disziplin Standarderfüllung hat es die Telekom Austria schon zu wahrer Meisterschaft gebracht. Sie ist nicht nur nach dem Informationssicherheitsstandard ISO 27001 zertifiziert, sondern erfüllt auch die Anforderungen von Sarbanes Oxley (SOX) und dem IT-Governance-Standard COBIT. Normen und Regulatorien sind eine Möglichkeit, sich dem Thema Sicherheit ganzheitlich zu nähern. Die Sinnhaftigkeit solcher Sicherheitsstandards ist allerdings nicht ganz unumstritten. Der streitbare Alemanne Alge sieht in ihnen sogar ein Sicherheitsrisiko (siehe Interview).

In jedem Fall tragen sie aber zur Bewusstseinsbildung bei, dass das Thema Sicherheit nicht nur eine IT-Angelegenheit ist, sondern eine Frage sicherer Prozesse von der Vorstandsetage bis hinunter zum Portier. Denn eines ist klar: Solange Passwörter auf Bildschirmen kleben oder Papiere mit sensiblen Informationen im Ausgabefach des Druckers liegen, wenn abends die Putzkolonne anrückt, hilft das teuerste Security-Equipment nichts. ❏

„Der Security Markt boomt weiterhin." - IDC-Österreich-Geschäftsführer **Joachim Seidler**

„Für uns ist ganz klar, dass ITdesign bei uns komplett als Betreuer auftritt", so Hanspeter Petschenig, Petschenig glastec, zum Wechsel auf eine homogene, stabile Linux-Landschaft und zur Komplettvernetzung über VPN. Zufriedene Kunden – oberstes Ziel von ITdesign, dem unabhängigen Dienstleister auf dem österreichischen IT-Markt.

www.itdesign.at

ITdesign
software projects & consulting

Check Point Experience 2007

Vor rund 1.000 Teilnehmern - mehr als doppelt so vielen wie im Vorjahr - präsentierte Check Point auf seiner alljährlichen Partner- und Kundenkonferenz namens CP Experience neue Produkte und die Richtlinien der Unternehmensstrategie. Das Motto für die Zukunft: „Pure Security".

Dunja Koelwel

Nokia IP2450, High-End-Sicherheits-Appliance für Firewall/VPN-Lösungen

Gil Shwed, Chairman & CEO von Sicherheitsspezialist Check Point, ging auf der diesjährigen Kunden- und Partnerkonferenz CX Experience 2007, die in diesem Jahr in München stattfand, gleich in medias res: „Fünf Schlagworte kennzeichnen Check Point", erklärte er zum Auftakt seiner Keynote, und diese seien Kontinuität, Konsistenz, Offenheit, Innovation und all das führe zum fünften Schlagwort, der so genannten Pure Security, dem Slogan unter dem die diesjährige Konferenz stand. Erstes und zweites Kriterium sei dadurch gewährleistet, dass Check Point seit 1993 immer dasselbe Geschäftsmodell verfolgt habe, nämlich IT-Sicherheit. Offenheit stehe für Systeme, die sich an jedes Unternehmen anpassen, Innovation habe man in der Vergangenheit bewiesen und wolle das weiterführen und Pure Security sei das Cover, das alles abdecke.

Pure Security

Wie Gil Shwed weiter ausführte, müsse Sicherheit heute auf unterschiedlichen Ebenen im Unternehmen stattfinden. Ein Durchschnittsunternehmen habe meist mehr als 15 verschiedene Sicherheitsdienstleister, die aber nicht wirklich effektiv seien, weil die Administration viel zu komplex im Alltagsleben sei. Daher ist nach Auffassung von Shwed der Fokus auf „Pure Security" wichtig. Konkret bedeutet das für den Check Point-Chairman, dass eine Sicherheitslösung Netzwerkattacken abfangen kann, das Eindringen von Malware verhindert, PCs, Mobile Devices oder auch Remote Access absichert und dies alles gemäß den entsprechenden juristischen Regeln.

Doch auf diesem Status quo will sich Check Point nicht ausruhen. Das Ziel ist die sogenannte End-to-End-Sicherheit, die Strategie der „Pure Security" der erste Schritt dazu. End-to-End-Sicherheit bedeutet dabei für Check Point zum einen eine 100%ige Verschlüsselung, die allgemein höchsten anerkannten Sicherheitszertifizierungslevel sowie „Zero Click Operations"-Sicherheit im Unternehmen, ohne dass Zusatzschritte erforderlich seien. Und last but not least soll diese Sicherheit auf allen Plattformen verfügbar sein.

Kein Mangel an Announcements

Was gab es noch bei Check Point? Natürlich jede Menge Announcements. Das spannendste dabei ist die Kooperation von Check Point, Intel und Nokia. Die drei Unternehmen wollen künftig gemeinsam an der verstärkten Absicherung der Unternehmensnetzwerke arbeiten. Ziel ist es, Unternehmenskunden neue Sicherheitsplattformen anzubieten, die die Sicherheit von Unternehmen durch Prüfung des Netzwerkverkehrs in Multi-Gigabit-Umgebungen ermöglichen und noch intensiver nach Anzeichen von Angriffsversuchen suchen, ohne die Netzwerkleistung zu beeinträchtigen.

Das erste Ergebnis dieser Zusammenarbeit ist die neue Nokia IP2450 Sicherheitsplattform, eine integrierte High-End-Sicherheits-Appliance für Firewall/VPN-Lösungen. Auf technischer Ebene ermöglichen Nokia, Check Point und Intel durch Zusammenführen ihrer Innovationen in einem dreigliedrigen Ansatz die Nutzung der Netzwerk-Sicherheitsstruktur von Unternehmen im vollen Umfang.

Auf dem Weg zur End-to-End-Sicherheit: **Gil Shwed**, Chairman & CEO von Sicherheitsspezialist Check Point

Der Intel Xeon 5355 Quad-Core-Prozessor ermöglicht Sicherheitsplattformen noch eine Verwaltung hoher Datenverkehrsaufkommen auf CPU-Ebene. Die vor kurzem vorgestellte Check-Point-CoreXL-Lösung ist Teil der Open Performance Architecture und bietet Leistung auf Rechenzentrumsniveau mit strengen Sicherheitsprüfungen, die die Leistung von Multi-Core-Prozessoren nutzen. Nokia verbindet das eigene, für Sicherheitsaufgaben optimierte Betriebssystem Nokia IPSO und die Nokia-Netzwerkprozessoren-Innovation (Accelerated Data Path Card Multi-Processing) und bietet somit ein Lösungspaket auf einer IP-Sicherheits-Appliance an - unterstützt durch seinen weltweiten Service und Support.

Im nächsten Schritt plant Nokia zu Beginn des nächsten Jahres die Unterstützung von Check Point CoreXL auf der Nokia IP2450 und anderen Multi-Core-Plattformen. Auf dem Weg zur Vermarktung der Produkte planen die Unternehmen ab November in ausgewählten Ländern in Europa und im Nahen Osten die gemeinsame Durchführung von Sicherheitsbriefings.

www.checkpoint.com

„Der Mitbewerb tut sich verflucht schwer mit uns."

Wieland Alge, CEO und Mitgründer des Tiroler Firewall-Herstellers Phion, erzählte im MONITOR-Gespräch über die Schutzwürdigkeit der Kommunikation, den Business-Nutzen von Sicherheitsinvestitionen, die Gefährlichkeit von Sicherheitsstandards und wie Phion die „Komplexitätsbarriere" durchbrochen hat.

Sie fordern in Sicherheitsfragen einen Fokus auf Kommunikationssicherheit. Sind Daten- und Informationssicherheit falsche Ansätze?

Das wird dann ein natürlicher Teil davon, aber man darf sich nicht so definieren, sonst hat man den Blick schon zu weit eingeschränkt. Informationen schütze ich am besten, wenn ich sie irgendwo einschließe, aber so kann man kein Business betreiben. Die Analyse, was unter schützenswerte Information fällt, ist je nach Firma und Branche unterschiedlich, aber das Gemeinsame aller Unternehmen ist, dass sie wie verrückt kommunizieren. Wenn man sich auf den Schutz von Daten und Informationen konzentriert, implementiert man unvollständige Prozesse. Außerdem kommt man beim Vorstand nicht mehr durch, wenn man immer wieder Geld für Information Security ausgeben will. Für den Schutz der Kommunikation bekommt man das Geld viel leichter, weil das einen tatsächlichen Business-Nutzen bringt.

Gibt es bei Security-Investitionen einen kalkulierbaren Return on Investment?

Welchen ROI hat eine Brandmeldeanlage? Wenn es nicht brennt, keinen. Da kann man keinen Business-Nutzen errechnen. Es wird jetzt viel diskutiert, wie IT und in weiterer Folge Security evident zum Business-Nutzen beitragen kann. Wenn es nicht evident ist oder erst herbeiargumentiert werden muss, dann ist es wahrscheinlich auch nicht so. Aber es gibt einen ROI beim Schutz der Kommunikation, zum Beispiel, indem ich Security-Technologien einsetze, um Leitungen effizienter zu nutzen und damit Leitungskosten zu sparen, oder indem ich Produktionsausfälle vermeide.

Sie sind auch ein großer Kritiker von Standards und Regulatorien wie SOX oder ISO 27001. Was stört sie daran.

Regulatorien sind eine konkrete Bedrohung der Security. Ihre Umsetzung kostet viel Zeit und Geld und bindet die besten Mitarbeiter. Wer beim Audit dann lauter grüne Hakerln hat, soll ja nicht glauben, dass er sicher ist. Das heißt nur, er hat eine Sache richtig gemacht, aber nicht notwendigerweise alle anderen. Wichtige Dinge werden versäumt, nur weil sie nicht im Framework der Norm drinnen stehen. Viele Unternehmen sind in einem merkwürdig unreifen Zustand, sie investieren viel Geld für wenig Nutzen - vor allem die ganz Großen. Aber dort fallen die Kosten nicht in Gewicht. Im österreichischen oberen Mittelstand macht es dagegen einen massiven Unterschied, ob ich IT effizient einsetze. Man muss sich die Frage stellen: Ist Security ein notwendiges Übel oder schaue ich, dass ich daraus einen Business-Nutzen gewinne?

Jetzt zu Ihrem eigenen Business: Die Security-Produkte von Phion haben Ihrer Meinung nach im Bezug auf Management-Architektur und Skalierbarkeit einen klaren Vorteil gegenüber dem Mitbewerb. Warum?

„Welchen ROI hat eine Brandmeldeanlage? Wenn es nicht brennt, keinen. Da kann man keinen Business-Nutzen errechnen." - **Wieland Alge**, CEO Phion

Phion entstand vor acht Jahren aus dem damals wahrscheinlich größten Firewall-Projekt der Welt im Allgemeinen Rechenzentrum in Innsbruck und Wien. Die Herausforderung war, zu zweit 600 Firewalls auszurollen und dann auch mit dem gleichen Personalaufwand zu betreiben. Das war in puncto Effizienzanforderung um den Faktor zehn bis 20 größer als alles, was am Markt vorhanden war. Da kann man nicht mehr quantitativ verbessern, sondern muss etwas vollständig Neues erfinden: Mit dem marktüblichen Umbrella-Management standen wir vor der Zahl 25 wie vor einer Schallmauer. Um diese Komplexitätsbarriere zu überwinden, wurde bei uns die Management-Plattform das Fundament der Lösung, auf dem Architektur und in weiterer Folge Funktionalität aufsetzen. Die Konkurrenz tut sich damit verflucht schwer. Die müssten alles Bisherige noch einmal neu erfinden. Unsere Lösung kann man nicht einfach als klügeres Umbrella-Management nachbauen. ❑

FOR YOUR **USB**-EYES ONLY!

CryptoPro Secure Device
Die Datenschutzlösung für USB-Speicher

CryptoPro Secure Device verschlüsselt USB-Speicher sicher und komfortabel.

- Einfach verteilt, schnell und kostengünstig implementiert.
- Automatische Erkennung der USB-Speicher – je nach Policy gesperrt oder sofort hochsicher verschlüsselt (AES 256).
- Zugriff ohne Installation oder Administrationsrechte möglich, u.v.m.

www.cpsd.at Wildbergstr. 32, 4040 Linz,
T: +43 (0)70/781 584-0, F: +43 (0)70/781 584-98

cpsd
it services GmbH

schoeller network control Forum 2007

Das zwischen dem Café Landtmann und dem Burgtheater gelegene MOYA (Museum of Young Art) hat schoeller network control dieses Jahr als Location für das heurige „network control forum" gewählt.

Adolf Hochhaltinger

Michael Gruber, Geschäftsführer schoeller network control (l.), eröffnete die Veranstaltung

Originell die Begründung: „Wirklich innovative IT-Lösungen für die Bereiche Fehler-Analyse, Performance-Optimierung und IT-Sicherheit sind die technischen Kunstwerke unserer Zeit."

Seit nunmehr zehn Jahren veranstaltet schoeller network control alljährlich dieses Forum mit internationalen Top-Referenten renommierter Hersteller und Partnerfirmen, es gilt inzwischen als etablierte Plattform zur Informationsbeschaffung und zum Erfahrungsaustausch für IT-Manager und Netzwerk-Verantwortliche. Die Veranstaltung stand diesmal unter dem Motto „Next Generation" und gab den Teilnehmern mehr Möglichkeiten, Vorträge ihres persönlichen Interesses zu besuchen.

„Das Informationsangebot war heuer noch breiter gefächert als in den Vorjahren und die Themen Performance-Analyse und Security spiegelten die aktuellen Trends für diesen Herbst wider. Der Schwerpunkt des Interesses lag bei den Themen Netflow Monitoring, Intrusion Prevention, resümiert Michael Gruber, Geschäftsführer schoeller network control, die Veranstaltung. „Wir konnten heute mit Brian Tolly von Spirent übrigens auch einen Vortragenden aus den USA begrüßen; er berichtete über den Nutzen von intensiven Testmethoden *vor* dem IT-Deployment. Gerade damit kann sich ein Unternehmen sehr viel Geld ersparen." Hier eine kleine Übersicht über einige der gebotenen Vortragsthemen.

Aladdin

Aladdin stellte die Authentisierungstechnologie „eToken" vor. Sie hat die Aufgabe, „nur die Guten" in das System zu lassen. Der „eToken" hat die Größe eines USB-Sticks und generiert jedes Mal einen neuen Einmal-Passwortcode, der nur dieses eine Mal gültig ist und auf einem LC-Display angezeigt wird. Seine Lebensdauer beträgt etwa fünf bis sieben Jahre.

Alternativ dazu hat der „eToken Pro" die Form einer Smartcard. Er wird zusammen mit einem Smartcard Reader geliefert, der an den USB-Port angeschlossen wird.

Alcatel Lucent

Mit dem Thema „Transaction Response-time Monitoring" befasste sich der Vortrag von schoeller / Alcatel-Lucent. Der Schwerpunkt dieses Vortrags lag beim Application Performance Monitoring. Dabei werden vor allem die vom Netzwerk geleistete Verfügbarkeit, Transaktionszeit und Antwortzeit ausgewertet.

„Ein ausgezeichnete Veranstaltung. Hier haben die Kunden einmal die Möglichkeit, die verschiedenen Anbieter zu treffen und mit ihnen zu sprechen, in einem etwas informelleren Rahmen als sonst üblich." - **Dave Lawton**, SE Manager EMEA bei Top Layer

Als Vorteile gelten hier die genaue Erfassung aller Transaktionen, das Verfahren dokumentiert das Verhalten direkt beim Anwender und erfasst alle User über verschiedenste Verbindungen. Bei SLA-Verletzungen erfolgt eine Alarmierung. Allerdings ist hierzu die Installation eines SW-Agenten auf den Clients erforderlich. Dafür werden sowohl Verzögerungen beim Client als auch Verzögerungen im Netzwerk aufgedeckt.

CheckPoint

Die beiden Stichworte Firewall und VPN (Virtual Private Network) kennzeichnen den Themenschwerpunkt von Checkpoint. Ein breites Portfolio bewährter und neu entwickelter Lösungen beweisen, dass man hier unter Netzwerksicherheit mehr versteht als „nur" Firewalling. Die Palette reicht von Verschlüsselung, Preboot Authentication und Recovery über zentrales Management bis zu Desktop Firewall und AntiSpyware.

Dabei werden sämtliche Wege beachtet, auf denen heute auf ein System zugegriffen werden kann, angefangen vom USB-Port (Kameras, externe Festplatten) über Netzlaufwerke, VPN Clients, SSL VPN bis hin zu File Sharing und FTP.

Fluke

Messtechnik-Spezialist Fluke präsentierte unter dem Titel „Network SuperVision" eine Übersicht über seine Geräte zur Analyse und Messung der Performance und der

technischen Eigenschaften eines Netzwerks - sowohl für Leitungen als auch für gesamte Netzwerke und für WLANs.

IBM / ISS

Das Netzwerk an vielen Stellen überwachen und anhand dieses Verhaltens die Unterschiede zwischen „braver" und „böser" Anwendung unterscheiden zu können - das ist der Ansatz von IBM / ISS. Das geschieht vor allem durch die Überwachungsgeräte der „Proventia"-Serie. Sie werden überall dort im Netzwerk installiert, wo man anhand des unterschiedlichen Verhaltens verschiedener Datenpakete eine Bedrohung am besten erkennen kann.

Ein wesentlicher Punkt ist, dass alle diese Geräte bei jeder neuen Bedrohung ein automatisches Update erhalten. Sobald eine neue Bedrohung auftritt oder eine neue Verwundbarkeit bekannt wird, entwickeln die Spezialisten von ISS schnellstens die entsprechenden Gegenmaßnahmen und spielen sie umgehend auf alle installierten Geräte auf - oft viele Monate bevor ein Hersteller des Betriebssystems endlich mit einem Patch darauf reagiert.

Juniper

Neben einer Vielzahl von Routing-Plattformen stellte Juniper seine Produktlinie skalierbarer Lösungen für integriertes Networking, Sicherheit sowie zur Beschleunigung von Anwendungen vor. Die Anwendungsbereiche reichen von Integrated Firewall/IPSec VPN über SSL VPN und Intrusion Prevention bis zur Zugangskontrolle sowie vom Load Balancing bis zur WAN Application Acceleration.

Network General

Das Aufspüren von Performance-Problemen in Netzwerken hat sich Network General zur Aufgabe gestellt. Dabei legt man neben dem Firefighting und Monitoring sowie Baselining, Anomaly Detection and Alarming besonderes Gewicht auf die forensische Analyse und auf die „Next-Generation-Fehlersuche" - umgesetzt durch die Produkte NetVigil, Visualizer und Sniffer InfiniStream.

Das Ergebnis: Anomalien im Auflauf des Netzwerks werden erkannt und durch Visualisierung der Log- und Überwachungsergebnisse sichtbar gemacht. Eine Besonderheit ist dabei die „Root-Cause Analysis", mit der auch über die *Ursache* der Störung konkrete Aussagen getroffen werden können.

RSA

Die Flut der unterschiedlichen Logfiles in einem Netzwerk zu bändigen und die für den Anwender wertvollen Informationen aus den Millionen Log-Zeilen herauszufiltern, hat sich RSA mit seinem Produkt „enVision" zum Ziel gesetzt.

„enVision" macht vor allem Jagd auf alle Log-Einträge, die in irgendeiner Form aus dem Rahmen fallen. So kann beispielsweise ein Trojaner entdeckt werden, sobald er versucht, mit seinem „Meister" Kontakt aufzunehmen - die (für dieses Netzwerk) unübliche IP-Adresse verrät ihn.

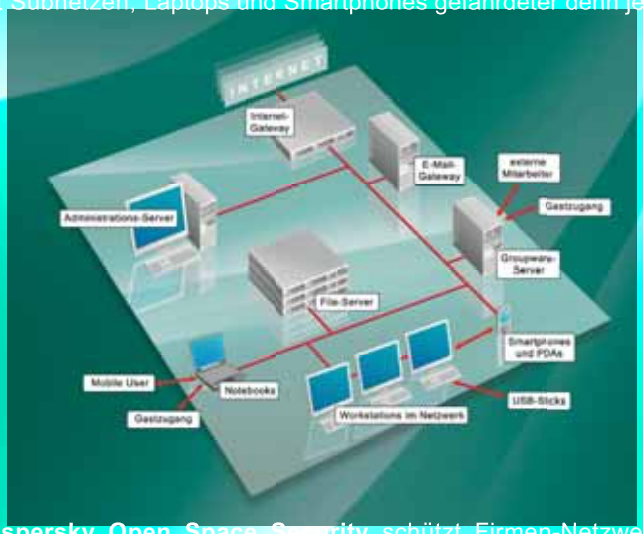
Ein Event Viewer visualisiert dabei das komplette Netzwerk und hebt potenzielle Probleme grafisch hervor.

Wesentlich sind dabei folgende Eigenschaften: Sicht auf *alle* Ereignisse im Netzwerk, Konzentration auf das „Wesentliche", schnelle Erkennung von Bedrohungen, schnelle Erkennung von Zusammenhängen und eine schnelle und angepasste (!) Reaktion auf Bedrohungen. In der Praxis wird dies durch die Korrelation der einzelnen Informationen und eine intelligente Auswertung der Gesamtsicht erreicht. ❑

KASPERSKY lab

Optimaler Schutz
für dynamische Unternehmens-Netzwerke

Firmen-Netzwerke sind offener und dynamischer geworden – doch mit Subnetzen, Laptops und Smartphones gefährdeter denn je.



Kaspersky Open Space Security schützt Firmen-Netzwerke jeder Größe inklusive externer Mitarbeiter und mobiler User zuverlässig – und wächst mit allen zukünftigen Anforderungen an die Unternehmens-IT.

Endlich sind Freiheit und Flexibilität sowie optimaler Schutz miteinander vereinbar.

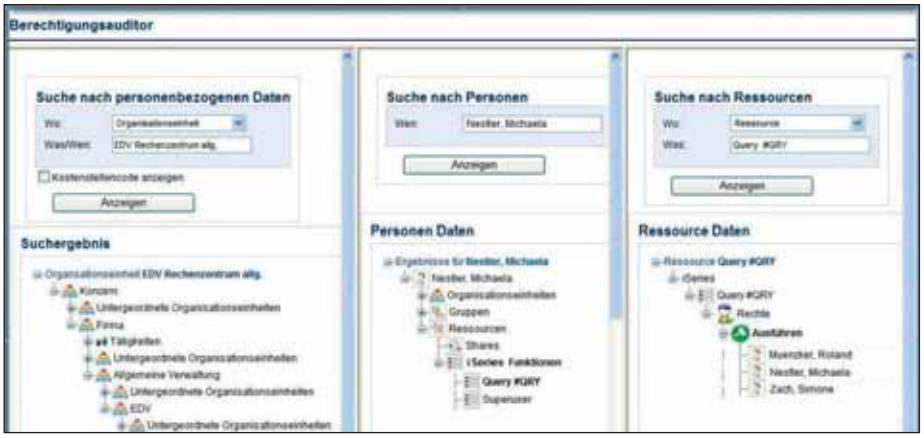
Kaspersky
Open Space
Security

- Optimaler Schutz vor Viren, Spyware und Hackern auf allen Netzwerk-Ebenen
- Proaktiver Schutz der Workstations
- Schutz von Mail- und File-Servern
- Echtzeit-Scan von Mails und Internet-Traffic
- Flexibel skalierbar
- Automatische Isolierung infizierter Clients und Verhinderung von Virus-Epidemien
- Zentrale Administration mit umfangreichem Berichts-System

www.kaspersky.at

„Mehr Compliance, mehr Sicherheit“

Unternehmen unterliegen vielen gesetzlichen und vertraglichen Regelungen, die zwingend eingehalten werden müssen. Auch die IT-Infrastruktur ist von diesen Regelungen betroffen. Mit dem „Berechtigungsauditor“ hat ITdesign eine Lösung entwickelt, die für Compliance-Maßnahmen eine wichtige Unterstützung bietet.



IT stellt nicht nur die Infrastruktur für Geschäftsprozesse bereit, sondern muss auch den Compliance-Anforderungen an das gesamte Unternehmen Folge leisten beziehungsweise dafür deren Einhaltung das nötige Rüstzeug liefern. Die Basis dafür bilden die Dokumentation interner Abläufe und Prozesse sowie entsprechende Kontrollsysteme.

Der Berechtigungsauditor (AudIT) ist eine Lösung, die es ermöglicht, die aktuellen Zugriffsberechtigungen auf Ressourcen unterschiedlichster Systeme übersichtlich und einheitlich darzustellen. Im Rahmen von Compliance-Maßnahmen hilft sie zunächst bei einer vollständigen Bestandsaufnahme sowie bei den daraus abzuleitenden Benutzerdaten-Bereinigungsaktivitäten. Darüber hinaus stellt sie die Basis für die Entwicklung von modernen Rollenkonzepten beziehungsweise rollenbasierendem Identitätsmanagement dar.

„Wer darf was?“

Im Zentrum stehen dabei Fragen nach den vorhandenen Ressourcen, dem verfügbaren Rechteportfolio, den Zugriffsberechtigungen auf diese Ressourcen, der Anwender und Anwendergruppen, die diese Ressourcen nutzen dürfen, den einzelnen Mitgliedern dieser Anwendergruppen und vieles mehr.

„Oft stellt sich erst im Zuge eines Compliance-Projektes heraus“, so Michael Botek, Geschäftsführer ITdesign, „dass Unternehmen für die Zuweisung von Rollen und Verantwortlichkeiten die notwendigen Basisdaten fehlen. Wer kann zum Beispiel dokumentieren, dass alle Abteilungswechsel oder Firmenaustritte von Mitarbeitern, in allen Systemen entsprechend den Sicherheitsvorgaben durchgeführt wurden? AudIT löst diese Anforderung.“

Mit einem Tool wie dem Berechtigungsauditor können diese Informationen erstmals aus unterschiedlichen Quellen zusammengefasst und dargestellt werden. Dabei kann es sich um Directories, Datenbanken, File Shares, Applikationen und anderem mehr handeln. So wurden beispielsweise, wie Botek erläutert, während eines aktuellen Rollenkonzept-Projektes Daten aus dem MS Windows File-System, MS Exchange, SQL Server, IXOS Archiv, IBM iSeries und einer Reihe von eigenentwickelten Applikationen ausgelesen.

Alle Berechtigungen im Griff

Das Herzstück des Tools ist eine SQL-Server-Datenbank, in welche die Daten importiert werden. Alle Informationen, die im Zusammenhang mit Berechtigungen stehen, sind hier von Belang:

- Gruppen: Active-Directory-Sicherheitsgruppen, Verteilerlisten, iSeries Benutzergruppen,
- Organisationseinheiten, deren Hierarchie und Mitglieder,
- Personen (alle in den Systemen vorhanden Accounts) und ihre Gruppenzugehörigkeit,
- Ressourcen (Files, Shares, Folders, E-Mail Accounts, iSeries-Programme und -Funktionen),
- Berechtigungen (Gruppen und Einzelpersonen) auf alle im System bekannten Ressourcen,
- Lokationen.

Nach abgeschlossenem Projekt werden über eine browserbasierte Darstellung den Verantwortlichen, die für die Bedienung keinerlei EDV-Wissen benötigen, auf einem Blick die gewünschten Informationen bereitgestellt.

Diese Informationen sind zugleich ein gutes Rüstzeug, um beispielsweise mit einem Identity-Management-Projekt den Sicherheitslevel, die Transparenz und die Nachvollziehbarkeit zu erhöhen. „Die zentrale Verwaltung von benutzerbezogenen Daten in Unternehmensnetzen bringt nicht nur Zeit- und Kostenersparnis, sondern ist auch ein wichtiges Sicherheitskriterium“, so Botek.

www.itdesign.at

Berechtigungsauditor (AudIT)

Der Berechtigungsauditor beantwortet u. a. folgende Fragen:

- Welche Ressourcen sind im System vorhanden?
- Welche Rechte sind für die Ressourcen vorgesehen?
- Wer hat welche Zugriffsberechtigung (z. B. Lesen, Ausführen, Vollzugriff ...)?
- Welche Gruppen sind in den Systemen angelegt?
- Wer ist Mitglied welcher Gruppe?
- Welche Gruppe hat auf welchen Ressourcen welche Berechtigungen?
- Wer gehört welcher Organisationseinheit an?

it & tel erweitert Housingfläche

Um der hohen Nachfrage an Server-Housing nachzukommen hat it & tel seine Housingfläche im Linzer TechcEnter verdoppelt.

it & tel-Housingfläche im TechcEnter Linz Winterhafen

Mit über 1.000 m² bietet it & tel in Österreich damit nun die größte Server-Housingfläche außerhalb Wiens an. Eingemietet sind hier die Server namhafter Unternehmen, darunter ein international tätiger Internetwettanbieter, einer der größten Kabelfernsehbetreiber oder ein weltweit agierender Telefondienstleister.

Die Vorteile von Server-Housing liegen in den Rahmenbedingungen. Für eine sichere Stromversorgung sorgen im TechcEnter Linz im Falle eines Stromausfalls zwei Notstromaggregate und zwei USV- Anlagen, die bis zum Anlaufen des Notstroms eine unterbrechungslose Versorgung sicherstellen. Mit einer Vollklimatisierung, vollautomatischen Brandlöschanlage, Zutrittskontrolle und Kameraüberwachung wird ein ideales Serverumfeld geboten.

it & tel ist das Telekommunikations-Geschäftsfeld der Elektrizitätswerk Wels AG.

Der Leistungsumfang erstreckt sich von Standortvernetzungen über Internet, E-Mail Dienste, Datensicherung, Security, Telefonkonzepten und Serverhousing bis hin zum Consulting. Das Unternehmen verfügt über ein eigenes Glasfasernetz in Österreich, der Slowakei, der Tschechischen Republik und Süddeutschland.
Kontakt: 07242-9396-7100;
www.ITandTEL.at

Kaspersky Lab erneuert „Zweitscanner“

Kaspersky Lab hat die neueste Generation von Kaspersky Anti-Virus Second Opinion Solution (S.O.S.) vorgestellt, deren Virenscanner auf den aktuellen Unternehmenslösungen von Kaspersky Lab basiert.

Unternehmen können damit ein zweistufiges Sicherheitskonzept umsetzen, so der Hersteller, indem sie Kaspersky Anti-Virus S.O.S. zusätzlich zu einem bereits installierten Virenscanner einsetzen und mit einem zweiten, unabhängigen Scan der Dateien die Sicherheit des Netzwerkes überprüfen. Da das Programm als reiner On-demand-Scanner konzipiert ist und keine Echtzeit-Schutz-Komponente enthält, arbeitet es mit vorhandenen Lösungen zusammen.

„Unternehmen erhalten einen großen Mehrwert, wenn sie die Leistung ihres Virenscanners durch einen zweiten überprüfen können, ohne zuvor die alte Lösung deinstallieren zu müssen“, ist Andreas Lamm, Geschäftsführer der Kaspersky Labs GmbH überzeugt. „Seit der Präsentation der ersten Generation unseres On-demand-Scanners vor einem Jahr wurden mehrere Unternehmen durch diese unabhängige Überprüfung ihres Netzwerkes überzeugt, auf Kaspersky-Lösungen umzusteigen.“

Die neue Version von Kaspersky Anti-Virus S.O.S. ist ab sofort über die Vertriebspartner von Kaspersky Lab zu beziehen.
www.kaspersky.com/de

Sind Sie sicher?

Wir bieten alles aus einer Hand

› USV
IT-Verfügbarkeit ohne Risiko

› Cooling
Perfektes Klima für High Performance Server

› Rack
Mehr Freiraum, Flexibilität und Sicherheit

› Security
Rundum-Absicherung der Infrastruktur

› Monitoring/Remote Management
Rechenzentrum: transparent und online

Rittal Schaltschränke Ges.m.b.H.
Wien – Linz – Graz – Lauterach
Tel. Zentrale: (01) 610 09-0
eMail: office@rittal.at
www.rittal.at

FRIEDHELM LOH GROUP

RITTAL

Bänderriss - wie Daten von Tapes gerettet werden können

Tapes spielen immer noch eine wichtige Rolle im Backupbereich, auch wenn ihre Zweckmäßigkeit durch Alternativ-Technologien wie SAN, NAS, Virtualisierung oder RAID-Systeme diskutiert wird. Gleich, welche Argumente die Gegner aufs Parkett bringen: Tape-Laufwerke und Libraries werden weiter benutzt.

Peter Böhret

Vor allem für die mittel- bis langfristige Archivierung haben Bänder immer noch Vorteile. Wer sich aber hier in scheinbarer Sicherheit wiegt, verlässt sich oft auf Laufwerke, die schon lange im Betrieb sind und deren Ausfall mit jedem Tag wahrscheinlicher wird. Der Vorteil der langen Lebensdauer von Tapes kann sich auch in das Gegenteil umkehren. Der üblicherweise angegebene Wert von 30 Jahren hängt nämlich von vielen Einzelfaktoren ab. Allein mit jeder Neubeschreibung steigt das Risiko, das Daten nicht mehr korrekt ausgelesen werden können. Das Ausmaß der Benutzung, die Qualität der Medien, die Wartung oder die Lagerung können schon vorher dazu führen, dass scheinbar unbeschädigte Tapes im Ernstfall nicht mehr verwertet werden können. Problematisch wird es auch dann, wenn der Hersteller des Backupformats nicht mehr am Markt vertreten ist.

Selbst die Schreib-/Leseverfahren an sich können durch die Belastung der Bänder mit jedem Vor- und Rückspulvorgang die Lebensdauer des Backups ändern und zum Beispiel zu verschleißbedingten Ausfällen des Mediums führen. Beim Helical-Scan entsteht eine große mechanische Belastung durch häufige Dehnung, Kopfjustage und große Kopfumschlingung. Lineare Aufzeichnungsverfahren dagegen erfordern ein mehrfaches Vor- und Rückspulen der Bänder. Auch die Anpassung der Datenübertragungsgeschwindigkeit kann eine Rolle spielen. Bei noch im Betrieb befindlichen Bändern mit ADR-Verfahren lässt sich deswegen die Schreibgeschwindigkeit stufenlos regulieren. Diese Medien passen sich damit automatisch der Datenrate an, die der Rechner überträgt, laufen daher kontinuierlich und müssen nicht ständig angehalten, zurückgespult oder neu positioniert werden. Das DLT-Verfahren achtet darauf, dass das Band nie von der Umlenkrolle und Spule auf der Datenseite berührt wird, sondern nur auf der Rückseite. Nur der Schreib-/Lesekopf kommt in Kontakt mit der Vorderseite.

Sobald es aber zum Datenverlust kommt, haben Spezialisten häufig eine Lösung parat. Eine Rettung von Tapes beruht vor allem darauf, die Daten mit Hilfe von modifizierten Laufwerken auszulesen und auf ein neues Medium zu überspielen. Diese Laufwerke können bei physikalisch oder logisch geschädigten Bändern gezielt die noch verwertbaren Sektoren des Bandes abspielen.

Datenrettungsmechanik in Reinraum und Labor

Selbst wenn Medien gerissen oder stark verschmutzt sind beziehungsweise großer Brandhitze ausgesetzt waren und das Gehäuse verformt ist, ist eine Rettung möglich. Grenzen setzt hier die Beschädigung der Trägerschicht oder die endgültige Überschreibung eines benötigten Backups. Selbst bei Brandschäden können häufig noch Daten gerettet werden, solange die Bänder nicht übertrieben ausgedehnt wurden und dadurch die Spuren verloren gegangen sind. Doch diese sind in der Regel erstaunlich resistent und selbst aus verschmolzenen Gehäusen können Informationen ausgelesen werden. Auch bei zerschnittenen oder zerknitterten Bändern können in den meisten Fällen Daten gerettet werden. Datenrettungsingenieure greifen mit Hilfe modifizierter Laufwerke auf noch intakte Teile des Bandes zurück und lesen die Informationen aus den noch intakten Bandteilen aus.

Dabei sind grundlegende, aber mit höchster Präzision durchzuführende mechanische Vorgänge Grundvoraussetzung für die Datenrettung. Ein durchschnittenes Band wird gespliced, das bedeutet, sauber geschnitten und die Reste zusammengeklebt. Danach werden diese Teile abgespielt und so viele Daten wie möglich ausgelesen. Nur die Bereiche, die physikalisch nicht mehr vorhanden sind, fehlen wirklich. Zerknitterte Bänder werden geglättet. Auch eine mikroskopisch sorgsame Reinigung ist ein wichtiger Faktor. Selbst kleinste Staubpartikel können zum Daten-

verlust führen. Sorgfalt und Schnelligkeit sind beim „Extremfall Wasserschaden“ zu beachten. Hier muss der Schmutz schnell durch Spülen entfernt werden, ehe er zwischen den aufgespulten Bandfilm kommt.

Bei physikalischen Beschädigungen ist bedeutend, welche Bereiche des Bandes in Mitleidenschaft gezogen wurden. Risse am Anfang oder am Ende des Bandes sind - je nach Backup-System - oft verschmerzbar, da hier der Verzeichnisbereich und nicht der Datenbereich betroffen ist. Auch in anderer Hinsicht bestimmt das Beschreibeverfahren die Erfolgsaussichten der Rettung: In Serpentinen beschriebene Bänder sind bei mechanischen Zerstörungen sehr schlecht wiederherzustellen. Hier werden die Bänder parallel in bis zu 100 Spuren beschrieben. Wenn es hier zu einem Riss kommt, sind sofort alle Spuren durchtrennt. Eine Rekonstruktion ist kaum noch möglich. Anders beim Helical-Scan, bei dem die Daten seriell aufgezeichnet werden. Ein Riss betrifft hier nur eine Spur und der Verlust ist somit automatisch viel geringer. Doch die Konstruktion der Bänder gleicht hier in der Praxis einiges aus. Parallel beschriebene Tapes sind in der Regel weniger mechanischen Belastungen ausgesetzt als seriell beschriebene. Letztere sind leichter zu bearbeiten, finden dafür häufiger den Weg in den Reinraum.

Bänderlogik

Doch auch bei mechanisch einwandfreien Kassetten kann es zu Fehlern kommen. Hier muss der Spezialist eine genaue Kenntnis der verschiedenen Methoden haben, nach denen die jeweilige Backupsoftware Dateien von einem Server oder einer Workstation auf das Band schreibt. Datenretter machen sich hier ihre Kenntnis der Beschreibungsmodi zu Nutze. Die jeweilige Backupsoftware überspielt Dateien von Festplatten in einem bestimmten Algorithmus als Datenstrom auf das Band. Die unterschiedlichen Formate zur Tapebeschreibung haben die verschiedensten Methoden, Daten einzulesen. Jedoch alle schreiben die Daten in Blocks festgelegter Länge auf das Band. Manche Formate platzieren ein zentrales Verzeichnis ans Ende eines Bandes, andere versehen jede Datei mit einem Header oder lagern ihr Inhaltsverzeichnis gleich auf die Festplatte des Servers aus.

Probleme einer Festplattenrettung, die durch Zerstörung einer zentralen Verzeichnisdatei, wie etwa der Master File Table entstehen, sind im Tape-Bereich nicht einschlägig. Festplatten können flexibel quer über alle Sektoren einer Platte ihre Informationen verteilen. Ist das Verzeichnis verschwunden, macht man sich hier dann aufwändig auf die Suche nach den Dateien, zum Teil Bit für Bit durch Auslesen auf Ebene der Hexadezimalcodes. Bänder schreiben alles nacheinander auf und erleichtern in dieser Hinsicht die Arbeit. Nach dem Auslesen stehen bei der Bänderrettung zudem die Signaturen der Backup-Software zu Hilfe. Mit Filtern lässt sich somit schnell nach einzelnen Dateien suchen. Fatal kann sich bei einem Band ein versehentliches Formatieren auswirken, was bei einer Festplattendatenrettung eher eine der leichteren Übungen ist. Denn auf das Band wird nun eine Tapemark geschrieben, die es, je nach Tape-Beschreibungsverfahren, nicht mehr mit herkömmlichen Mitteln erlaubt, das Band auszulesen. Nun muss tief in die Hardware eingegriffen und sogar an der Firmware des Herstellers gearbeitet werden. Bei diesem so genannten Re-Engineering ist in jedem Fall Entwicklungsarbeit nötig. Datenrettungsspezialisten von Kroll Ontrack forschten beispielsweise ein halbes Jahr, ehe ein standardisiertes Verfahren für DLT-Medien zur Verfügung stand. Auch Tape-Libraries können gerettet werden. Der Verlust des ersten Bandes oder einzelner späterer Bänder beeinträchtigt hier nicht das Auslesen der übrigen Daten im Labor. Auch hier tun die modifizierten Laufwerke ihre Dienste.

Konvertierung als Zukunftsaufgabe

Datenrettung bei Tapes wird lange wichtig bleiben. Denn immer noch sind wichtige Daten auf Bändern vorhanden. Vor allem im öffentlichen Sektor und im archivarischen Umfeld müssen Informationen auch noch in Zukunft zur Verfügung stehen. Konvertierung alter Bänder in neue Formate ist hier ein wichtiges Thema. Datenretter mit ihrem Praxis-Know-how sind gefragte Männer, wenn es zum Beispiel um die schrittweise Konvertierung von Bändern aus einem Bestand von bis zu 50.000 Tapes geht. ❑

www.ontrack.at

Bestellen Sie jetzt bei Ihrem österreichischen Distributor!

ACTEBIS AME GROUP POINT INGRAM MICRO OMEGA computer laser systeme

MGE Office Protection Systems bietet Ihnen Tower-Geräte der Line-Interactive USV-Serie Evolution zu einmaligen Sonderpreisen!

Evolution 850 VA	68452	165 €
Evolution 1150 VA	68454	235 €
Evolution 1550 VA	68457	315 €
Evolution 2000 VA	68460	475 €

Gewinnen Sie eine Reise zur Fußball Premier League nach London! Wir laden Sie ein! Seien Sie unser Gast! Infos bei Ihrem Distributor oder bei MGE Office Protection Systems +49 2131 3593-206.

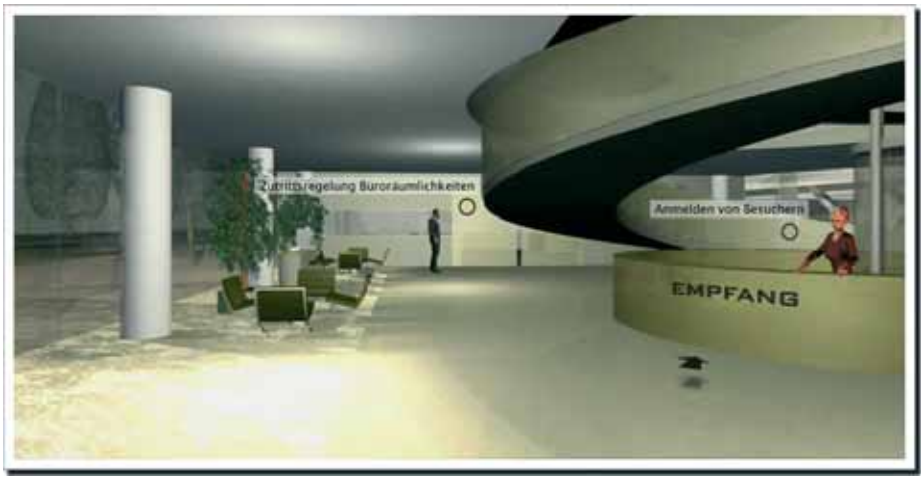
MGE Office Protection Systems

© appeal 025 710

„Sicherheitsbewusstein kann man lernen“

Wie können Unternehmen das Sicherheitsbewusstsein ihrer Mitarbeiter steigern? MONITOR sprach darüber mit Christian Brandl, Geschäftsführer des Tiroler IT-Unternehmens E-SEC Information Security Solutions GmbH.

Dominik Troger



Sicherheitsbewusstsein lernen im „virtuellen Büro“.

Viele sicherheitsrelevante Vorfälle in Unternehmen werden von den eigenen Mitarbeitern generiert.

Rund 65% aller sicherheitsrelevanten Vorfälle in Unternehmen werden - meist unwissentlich - durch die eigenen Mitarbeiter verursacht. Je sicherer technische Systeme werden, desto mehr wird der Mensch zu einem zentralen Risikofaktor. Vor allem dann, wenn er immer komplexeren Anforderungen im täglichen Arbeitsleben gewachsen sein muss.

Welche Sicherheitslücken sind hier vorherrschend?

Das reicht von Fehlbedienungen über mangelndes Sicherheitsbewusstsein bis hin zu absichtlicher Schädigung unternehmenseigener Daten und Systeme. Eine weitere Sicherheitslücke stellt die zunehmende Mobilität der Mitarbeiter dar.

Um wichtige Informationen und sensible Daten vor unwiederbringlichem Verlust oder unberechtigtem Zugriff wie Industriespionage und Social Engineering zu schützen, müssen die Mitarbeiter daher als ganz wichtiger Faktor einer integrierten, unternehmensweiten Informationssicherheit berücksichtigt werden.

Welche Mitarbeitergruppen sind davon betroffen?

Das beginnt schon beim Empfang und der Zutrittsregelung für die Büroräumlichkeiten und schließt alle Mitarbeitergruppen ein - von der Geschäftsleitung über die Systemadministratoren und IT-Spezialisten bis hin zu den Anwendern.

Hat es nicht auch mit einem mangelnden Sicherheitsverständnis der Mitarbeiter zu tun?

Wenn man Mitarbeitern nur ein Handout in die Hand drückt, werden sie nicht verstehen, warum sie Teil einer unternehmensweiten Sicherheitsstrategie werden sollen und sie fühlen sich in ihrer Arbeit eingeschränkt. Ein Risikofaktor sind auch neue Mitarbeiter, die über dieses unternehmensinterne Sicherheitswissen noch nicht verfügen können.

Wie können Unternehmen das Sicherheitsbewusstsein der Mitarbeiter heben?

Zwar ist das Bewusstsein für den „Risikofaktor“ Mitarbeiter in den letzten Jahren gestiegen - Projekte im Bereich Security Awareness verlaufen aufgrund unklarer Kompetenzverteilungen aber oftmals im Sande.

Voraussetzung für eine umfassende Informationssicherheit ist daher eine klare Regelung, wer für die Erstellung und Einhaltung der Security Policy verantwortlich ist und welche Rechte und Pflichten die einzelnen Mitarbeiter haben.

Was ist das Ziel solcher Maßnahmen?

Ziel ist es, einerseits das Bewusstsein der Mitarbeiter, aber auch deren Fähigkeiten und Kenntnisse in puncto Informationssicherheit zu stärken sowie andererseits aktuelle Sicherheitslücken aufzudecken und die Anzahl von Sicherheitsvorfällen zu minimieren. Die Mitarbeiter sollen in die Lage versetzt werden, kritische Situationen zu erkennen und die richtigen Maßnahmen zu ergreifen.

Welche Hilfestellungen bieten Sie hier?

Nachdem nur Maßnahmen und Verhaltensweisen, welche von den Mitarbeitern verstanden werden, im Gedächtnis bleiben und dem Mitarbeiter im Ernstfall helfen, richtig zu handeln, haben wir als Unternehmen einen ganz neuen Ansatz gewählt: die multimediale und interaktive Aufbereitung von Richtlinien und grundlegenden Verhaltensweisen im Rahmen eines „virtuellen Büros“. Dieses Konzept umfasst auch ein Security-Portal, das den Mitarbeitern als zentrale Informationsstelle zu Sicherheitsthemen (Glossar, Richtlinien, FAQs etc.) dient und vom Unternehmen laufend aktualisiert werden kann.

Die Software deckt somit sämtliche Security-Awareness-Aspekte ab und kann optional durch das Absolvieren eines Online-Tests abgeschlossen werden.

www.e-sec.at

Security Awarness im Komplettpaket

E-SEC Information Security Solutions GmbH mit Sitz in Innsbruck wurde im Jahr 2005 gegründet. Die Entwicklung des Konzepts für die Einführung, Erhalt und die Verbesserung von Security-Awareness-Maßnahmen und der dafür eingesetzten, unterstützenden Software startete bereits 2003 im Zuge eines Projektes an der Technischen Universität Innsbruck. Zu den Referenzen zählen u. a. Raiffeisen Rechenzentrum Tirol GmbH , Skidata AG und die PlanseeGroup.

E-Mails ohne Viagra

Sicherheitslösungen von Kapsch und SonicWALL erkennen rechtzeitig Gefahren und hüten so die elektronische Kommunikation.

Die meisten Unternehmen im KMU-Bereich müssen ihre IT-Ressourcen vor Angriffen einfach und zu vernünftigen Kosten schützen. Ein ganzheitlicher Lösungsansatz mit sogenannten vorausschauenden Techniken gewährleistet ausreichend Sicherheit, da Gefahren in eingehenden E-Mails erkannt und Anomalien in ausgehenden E-Mails gleichzeitig geortet werden. Spam oder Phishing sowie dem Diebstahl von Unternehmensdaten oder unbeabsichtigter externer Weiterleitung persönlicher Daten wird somit effektiv begegnet.

Eine neue Sicherheitslösung ist heutzutage innerhalb von kürzester Zeit voll funktionsfähig und administrierbar. Sie schließt Sicherheitslücken bei sendenden Servern, E-Mail-Inhalten, Anlagen, eingebetteten URLs und Websites etc. und differenziert bösartige Inhalte ebenso wie Angriffsarten. Filter sind dabei immer detaillierter anzulegen, um abgewandelte Begriffe abzuwehren.

Das Wort „Viagra" greift z. B. mittlerweile mit 600.426.974.379.824.381952 Varianten an. In einer Internet-Umgebung ist auch die Server-Authentifizierung ein komplexer Vorgang, damit „gute" E-Mails auch weiterhin durchgelassen werden. Ein kombinierter Ansatz von Techniken lässt den Status mit größerer Genauigkeit bestimmen.

Kapsch als führender Security-Anbieter realisiert diese kombinierten Sicherheitslösungen mit dem Partner SonicWALL, einem international führenden Hersteller von Lösungen für Unternehmen jeder Größe im Bereich Netzwerksicherheit, Remote-Zugriff, Datenschutz, Web- und E-Mail-Sicherheit sowie Richtlinien- und Managementlösungen. ❑

„Eine ganzheitliche Security-Lösung von Kapsch und SonicWALL konsolidiert alle vorhandenen Systemteile und lässt sich auch mit einer geringen Anzahl Server umsetzen. Sie bietet schnellere Konfiguration, einfache Benutzeranpassung, webbasierende Oberflächen, automatische Updates und vieles mehr." - **Thomas Blaschka**, Produktmanager Security Solutions bei Kapsch

kapsch >>>

Mehr Infos unter www.kapsch.net, www.sonicwall.at

PROMOTION

KOMPETENZ VERBINDET. SCHRACK TECHNIK

NETZWERKTECHNIK – JETZT DEN NEUEN KATALOG ANFORDERN!

- CAT5 LINE STP
- DE-EMBEDDED LINE CAT6 STP
- TOOLLESS LINE KLASSE D, E, EA STP
- IP44 LINE
- FLEX LINE CAT6/7 STP
- EC7 LINE STP
- GG45 LINE STP
- ZUBEHÖR KUPFERVERKABELUNG
- TELEFONIE
- MESSGERÄTE
- LWL-VERKABELUNG
- AKTIVE KOMPONENTEN
- NETZWERKSCHRÄNKE
- USV-ANLAGEN

SCHRACK TECHNIK GMBH
Seybelgasse 13, A-1230 Wien
TELEFON +43(0)1 / 866 85-0, E-MAIL info@schrack.com

WWW.SCHRACK.AT

USV Serie SG-CE 80 bis 300kVA

Die SG-CE-Serie zählt zu den leistungsfähigsten und zuverlässigsten 3-Phasen-USV auf dem Markt. Sie bietet eine ausfallsichere Stromversorgung für zahlreiche Anwendungen.

Die SG-CE-Serie arbeitet im VFI-Modus (spannungs- und frequenzunabhängig) und wurde entwickelt, um die zunehmende Nachfrage nach Clean-Input-Leistung durch einen innovativen Kontrollalgorithmus in den IGBT-Gleichrichter-Komponenten zu erfüllen (anstatt Standardfilter zu verwenden). Die Entwicklung der SG-CE-Serie erfolgte nach der strengen GE-SixSigma-Methodik, um sicherzustellen, dass das Produkt den Kundenanforderungen vollständig entspricht.

Die USV der SG-CE-Serie bietet Zuverlässigkeit und Leistung auf höchstem Niveau. Durch eine Backfeed-Schutzschaltung und die Erfüllung von EMV- und Sicherheitsstandards entspricht die SG-CE-Serie den geltenden Normen. Die Zuverlässigkeit kann durch Parallelschaltung mehrerer Einheiten unter Einsatz der einzigartigen RPA-Technologie (Redundant Parallel Architecture) von GE noch gesteigert werden. GE bietet über den gesamten Lebenszyklus hinweg Unterstützung durch seine Serviceteams, mit zentraler Hotline, lokalem Support rund um die Uhr und flexiblen, an Bedürfnisse und Budget angepassten Service-Verträgen zur präventiven Wartung.

PurePulse: IGBT-Gleichrichter Clean Input Performance

Die USV der SG-CE-Serie von GE mit 160 bis 300 kVA sind wahlweise mit herkömmlicher Transformator-Gleichrichtertechnologie oder mit Gleichrichtern auf Basis der neuen PurePulse-Technologie von GE erhältlich.

PurePulse ist ein innovativer Kontrollalgorithmus, der auf den IGBT-Gleichrichter angewendet wird. Dieser Stromquellen-Gleichrichter gewährleistet einen Eingangs-Klirrfaktor (THDi) von unter 2% und erzeugt am Ausgang eine rein sinusförmige Kurve.

Die Vorteile der PurePulse-Technologie von GE reichen von Einsparungen bei der Dimensionierung der vorgeschalteten Komponenten (wie Generatoren, Verkabelung und Unterbrecher) bis zum völligen Wegfall von Kosten für weitere aktive oder passive Eingangsfilter.

PurePulse ist eine bahnbrechende Innovation von GE.

Kontakt: **General Electric Austria GmbH**
Donaucitystraße 6/3. Stock, 1220 Wien
+43 1 260 16–250
sales-ups.at@ge.com

PROMOTION

Spannungsschutz für Server

Die flachgebauten Anlagen der USV-Serie Ellipse MAX sind in einem Leistungsbereich von 600 VA bis 1500 VA erhältlich. Sie ersetzen die USVs der bisherigen Ellipse Premium-Serie.

Die Produktfamilie der Ellipse MAX ist mit Advanced Surge Reduction (ASR) ausgestattet. Diese Funktion entspricht der IEC-Norm 61643-1 und ermöglicht für sensible Workstations und Server einen kostengünstigen Überspannungsschutz. Die Geräte sind speziell für den Einsatz in kleinen und mittleren Unternehmen konzipiert und bieten Überspannungsschutz, Line-Interactive-Technologie und die Möglichkeit zum Einsatz im 19"-Rack mit zwei HE. Die flache Bauform ermöglicht die Installation unter einem Monitor, in vertikaler Position als Tower-Modell. Die Ellipse MAX ist in fünf Modellen von 600 bis 1.500 VA erhältlich.

MGE Office Protection Systems

Im Februar dieses Jahres wurde der Zusammenschluss von MGE und APC unter dem Dach des französischen Konzerns Schneider Electric durch die Europäische Kommission unter der Auflage genehmigt, das USV-Geschäft von MGE 0-10 kVA eigenständig zu betreiben.

Aus dieser Entscheidung geht MGE O. P. SYSTEMS hervor, die neue Marke für den Vertrieb der einphasigen USV- Anlagen und Überspannungsschutzprodukte von MGE UPS SYSTEMS. MGE O.P. Systems tritt rechtlich die Nachfolge von MGE UPS Systems an.

Ab sofort sind unter dieser Marke die MGE-Überspannungsschutzprodukte der Typen Protection Box und Protection Center, sowie die einphasigen USV-Systeme Ellipse ASR, Evolution/Evolution S, Pulsar, Pulsar M, Pulsar MX (bis 20 kVA) und Comet EX RT erhältlich.

Außerdem ist diverses Zubehör im Produktportfolio von MGE Office Protection Systems enthalten. Abgerundet wird die Produktpalette durch die USV-Management-Software „Solution Pac".
www.mgeups.at

Professionelle USV-Lösungen

Die Abhängigkeit des Menschen von Computern, Telekommunikationsanlagen und anderen elektronischen Einrichtungen steigt permanent an.

Powerware 9395 von Eaton: jetzt auch mit leistungsstärkeren Modellen mit 450 und 550 kVA

Die unterbrechungsfreie Verfügbarkeit des Stromnetzes sowie die notwendigen Stromwerte können von den Energieversorgungsunternehmen nicht immer konstant aufrechterhalten werden. Speziell kritische Anwendungen wie computergesteuerte Prozesse in Krankenhäusern und Rechenzentren sind genau von dieser unterbrechungsfreien Verfügbarkeit in hohem Maße abhängig. Netzausfälle können enorme Kosten und Aufwände verursachen.

Um Betreibern von USV-Anlagen die Wahl von Anfang an zu erleichtern, bietet KESS ein beliebig erweiterbares USV-System an. Der modulare Aufbau der KESS USV Conceptpower ermöglicht eine einfache Erweiterung und das System wächst mit Unternehmen. Es wird eine Fehlertoleranz von n+1 gewährleistet. Durch einen Wirkungsgrad von 96% im Online Mode sollen die Kosten von Klimatisierung und Stromverbrauch reduziert werden.

Die neue PW9395 von Eaton verfügt über einen Leistungsbereich von 225-550 kVA. Durch eine aktive Powerfaktorkorrektur wird der Klirrfaktor bei 3-5% so gering wie möglich gehalten.

Das bedeutet, so der Hersteller, Zuverlässigkeit, Verfügbarkeit und hohe Performance. Die Anlage eignet sich beispielsweise zum Schutz von Netzwerken in der industriellen Automatisierung und anderen unternehmenskritischen Anwendungen wie beispielsweise Serverfarmen, Gebäudemanagementsystemen, Datenzentren und medizinischen Einrichtungen.

www.kess.at

Triple AcceSSS IT Distributions & Dienstleistungs GmbH
Brown Boveri Str. 6 Top 15/16
A-2351 Wr. Neudorf

t: +43 (0) 2236 864444 - 0
f: +43 (0) 2236 864444 - 4

office@3xs-it.com
www.3xs-it.com

3xS-it.com

Rufen Sie unter 02236/86 4444 – 8 an oder schreiben Sie ein Mail an trend_webthreats@3xs-it.com und gewinnen PC Cillin Internet Security zum Schutz Ihres PCs!

Hersteller	Produktname	Leistung in kVA	Technologie nach IEC 62040-3 Stufe 1 ❶	Spannungskurvenform des USV-Ausgangs nach IEC 62040-3 Stufe 2 bei		Dynam. Toleranzkurven des USV-Ausgangs nach IEC 62040-3 Stufe 3			Besonderheiten	Endpreis inkl. USt in €	Bezugsquelle
				Normalbetrieb ❷	Batteriebetrieb ❷	bei Ändern der Betriebsart ❸	bei linearem Lastsprung ❸	bei nichtlinearem Lastsprung ❸			
Ablerex	Mars MS6000	6	VFI	S	S	1	1	1	Parallelschaltbar für redundanten Betrieb, Slot für Kommunikationseinschübe, Batterieerweiterungsmöglichkeit	1.990,-	RGE Robert Gmeiner Tel. 02256/65954-0
Ablerex	Mars MS1000RT	1	VFI	S	S	1	1	1	Als Rack- oder Standmodell verwendbar, Slot für Kommunikationseinschübe, Batterieerweiterungsmöglichkeit	530,-	
Ablerex	Vesta VT625	0,625	VI	S	Y	3	3	3		90,-	
Aros	e-Sentinel	0,5 bis 2	VI	S	S	3	1	1	Die USV ist auch als 19"-Version verfügbar, minimaler Verbrauch - hoher Wirkungsgrad, Überspannungsschutz für Telefonleitungen (RJ45/RJ11), SNMP Slot zur Anbindung der USV-Anlage an das EDV- Netzwerk, kostenlose Shutdown Software	ab 330,-	Schmachtl Tel. 01/616 21 80-0
Aros	Flexus	10 bis 20	VFI	S	S	1	1	1	Vollgraphischer Kontrollmonitor (114 x 64mm), Batterieerweiterungen bis zu mehreren Stunden, Kommunikationsslots für SNMP-Schnittstelle etc., 6-fach parallelschaltfähig zur Erhöhung der Leistung bzw. aus Redundanzgründen, Ausgangsleistungsfaktor 0,9	auf Anfrage	
Aros	Sentinel XR	3,3 bis 6	VFI	S	S	1	1	1	Die Batterien können während des Inverterbetriebs ohne Störung der angeschlossenen Verbraucher getauscht werden. Die USV ist als 19" oder als Standversion einsetzbar. Digitales Display zur Anzeige von Messwerten, Auslastung, Störungen usw. SNMP Slot, kostenlose Shutdown-Software	ab 1.500,-	
Eaton/Powerware	PW 9395	ab 225	VFI	S	S	1	1	1	Parallelschaltbar, flexible Batteriekonfiguration, besonders für Einsatz in Industrie und IKT-Applikationen, viele Kommunikationsmöglichkeiten wie SNMP, Modbus, Relais, inkl. Software	auf Anfrage	KESS Power Solutions Tel. 01/470 47 31-0 RGE Robert Gmeiner Tel. 02256/65954-0
Eaton/Powerware	PW 9355	8 bis 40	VFI	S	S	1	1	1	Parallelschaltbar, THDi<5%, cosphi=0,9, Slot für Kommunikationseinschübe, Batterieerweiterungsmöglichkeit	auf Anfrage	
Eaton/Powerware	PW 9140	7,5 bis 10	VFI	S	S	1	1	1	19"-RackMount USV, 7,5 und 10 kVA mit nur 6 HE!	auf Anfrage	
Errepi	On Power 1503R	1,5	VFI	S	S	1	1	1	19"-Rackausführung, RS232 und USB, steckfertige Batterieausweitung	auf Anfrage	Syscom GmbH Tel. 01/732 29-0
Kess	KESS-USV Concept-power Modular	10 bis 40	VFI	S	S	1	1	1	Modularer Aufbau, einfache Aufrüstung für Redundanz und Leistungserweiterung	auf Anfrage	KESS Power Solutions Tel. 01/470 47 31-0
General Electric	LP-Serie	3 bis 120	VFI	S	S	1	1	1	Hoher Ausgangsleistungsfaktor & Überlastfähigkeit, elektronischer Netz-Bypass, Handumgehung, LCD-Anzeige, Superior Battery Management, ECO-Modus, RS 232 inkl. USV-Server-Shutdown-Software Datashield auf Java-Basis, optional: Parallelbetrieb, Batterieerweiterungen u. a.	auf Anfrage	General Electric Tel. 01/26016-250
General Electric	SitePro & SG-Serie	10 bis 500	VFI	S	S	1	1	1	Neueste PurePuls-Technologie (clean input) mit THDi <3%, hoher Ausgangsleistungsfaktor und hohe Überlastfähigkeit, galvanische Trennung mittels Ausgangstransformator, elektronischer Netz-Bypass, Handumgehung, Superior Battery Management, ECO-Modus, RS 232 inkl. USV-Server-Shutdown-Software	auf Anfrage	
General Electric	VH	0,7 bis 3	VFI	S	S	1	1	1	3 Jahre Garantie auf Elektronik und Batterie, Einsatz als Tisch-und 19"-System sofort möglich, nur 2 HE für alle Leistungen, statischer Bypass, USB, weites Eingangsspannungsfenster 160-280 V, einfacher Batterietausch während des Betriebs möglich, inkl. USV-Server-Shutdown-Software auf Java-Basis	auf Anfrage	
OptiUPS	ES800C	0,8	VI	S	S	3	3	3	Robuste Ausführung mit Trafo, viele Optionen verfügbar	190,-	RGE Robert Gmeiner Tel. 02256/65954-0
Meta System	Trimod 10	10	VFI	S	S	1	1	1	Modular erweiterbar, Redundanzlösungen, 1- oder 3-phasig verwendbar, Slot für Kommunikationseinschübe, Batterieerweiterungsmöglichkeit	6.220,-	
MGE Office Protection Systems	Evolution	0,65 bis 3	VFD	S	S	3	1	3	Best Deal, 1.150VA ab 330 Euro, netzwerk-fernwartungsfähig, powershare - programmierbare Steckdosen	ab 230,-	MGE Office Protection Tel. 01/617 44 12
MGE Office Protection Systems	Ellipse MAX 1500	0,6 bis 1,5	VI	S	Y	3	1	3	Lüfterlos, Wand- und 19"-Montage optional, netzwerkfähig und fernwartungstauglich über Proxy	ab 120,-	
MGE Office Protection Systems	Pulsar	0,7 bis 20	VFI	S	S	1	1	1	Ab 2 kVA, modular erweiterbar, netzwerkfähig, drehbares Display für Anzeige von Messdaten und Steuerung (kein PC/Laptop) notwendig, auch passend für 600 mm Schränke	auf Anfrage	
Rittal	PMC 12	1 bis 2	VFI	S	S	1	1	1	19" Rack- und Standmontage, Batterielebensdauer 5 Jahre nach EUROBAT, zusätzliche Batteriepakete zur Erhöhung der Autonomiezeit, Batterien im Betrieb von vorne austauschbar, Redundanzbetrieb mittels Parallel Hot Swap Chassis möglich	ab 682,80	Rittal Tel. 01/610 09-0
Rittal	PMC 200	10	VFI	S	S	1	1	1	Modulartechnik bis zu 200 kW in einem Schrank, dezentrale Parallelarchitektur (reduntanter Schutz ohne Single Point of Failure), Hot-Swap-fähige-Module	auf Anfrage	
Schrack	usdd 3300 bis 10.000VA	3.300 bis10.000	VI	S	S	1	1	1	19-Zoll-Rackversion, inklusive der Funktion, off-line und Netzinteractive und der Funktion „smart aktiv", das ein intelligentes System zwischen Line Interactive und Double Conversion besitzt	auf Anfrage	Schrack Energiesysteme Tel. 01/86685-0

Symbolerklärungen:

❶ **VFD....**Offline/Standby - **VI....**Line Interactive/Single Conversion - **VFI**....On-Line, Double Conversion
❷ **S...**sinusförmig, **X....**nicht sinusförmig D>0,08 bei nichtlinearer Referenzlast, **Y**....nicht sinusförmig, überschreitet Grenzwerte von IEC 6100-2-2
❸ **1....**unterbrechungsfrei - **2....**Unterbrechung <1ms - **3....**Unterbrechung <10ms)

Sicherheit für Webanwendungen

Unternehmen, die Portalumgebungen oder Online-Shops betreiben, sehen sich einer wachsenden Gefahr ausgesetzt: Webanwendungen sind zum bevorzugten Ziel von Hackern und IT-Kriminellen geworden.

Peter Hanke

Um Webanwendungen zu manipulieren, benötigen Hacker meist weder umfangreiche Programmierkenntnisse noch spezielle Hilfsmittel. Und viele Webapplikationen sind nur ungenügend geschützt. Während Unternehmen bei Netzwerksicherheit und Virenschutz heute meist gerüstet sind, unterschätzen sie die Risiken von Webanwendungen nach wie vor.

Laut Security-Spezialist Symantec erfolgen vier Fünftel der Web-Angriffe über leicht ausnutzbare Schwachstellen. Zudem ermöglichen Webapplikationen direkten Durchgriff auf Backend-Systeme. Sensible Informationen wie Kundendaten oder vertrauliche Geschäftsunterlagen können so preisgegeben werden. Nach Expertenmeinung operieren Hacker immer häufiger gemeinsam mit der organisierten Kriminalität - hinter den Angriffen stecken oft konkrete wirtschaftliche Interessen, mit beträchtlichen Folgen für die Betroffenen. Denn neben der Störung der internen Prozesse droht massiver Imageverlust - und damit verbundene Umsatzeinbußen.

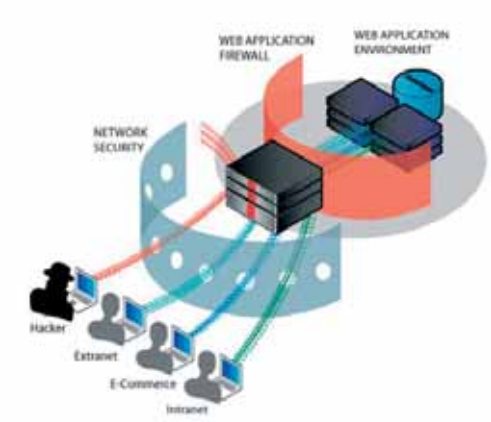
Traditionelle Konzepte reichen nicht

Dabei ergeben sich durch den Einsatz von Webanwendungen und Web-Services viele Vorteile. Immer mehr Unternehmen binden deshalb Partner, Dienstleister und Lieferanten online ein, auch Geschäfte mit Endkunden werden zunehmend so abgewickelt. Dass der Datenschutz bisweilen auf der Strecke bleibt, zeigt das Beispiel eines großen Versandhauses. Dort konnten Betrüger bis vor kurzem auf fremde Rechnungen online einkaufen. Dazu mussten Sie nur den Link „Passwort vergessen“ anklicken, und konnten sich dann als einer von mehreren Tausend Shops ausgeben, der dann die Rechnung für die Bestellung bekam. Aus technischer Sicht sind mehrere Herausforderungen zu bewältigen: Weil sie oft unter großem Zeit- und Kostendruck entwickelt werden, wird die Sicherheit nicht konsequent bedacht. Sicherheitslücken werden dann erst nachträglich geschlossen, während im Web täglich neue Bedrohungen aufkommen.

Die größten Gefahren drohen durch Angriffe auf Anwendungsebene - wie zum Beispiel SQL-Injection oder Cross-Site-Scripting. Traditionelle Sicherheitskomponenten wie Netzwerk-Firewalls und Intrusion-Detection-Systeme sind hier in der Regel machtlos. Sie „verstehen“ Anwendungs-Traffic auf Session- oder User-Ebene nicht, können Bösartiges nicht von normalem Verhalten unterscheiden. Und Hacker passen ihre „Waffen“ ständig neuen Konstellationen an. Auch die so genannten Zero-Day-Attacken - also Angriffe, für die noch keine Schutzmechanismen entwickelt wurden - gilt es abzuwehren.

Umfassender Schutz

Viele Argumente also für Web Application Firewalls - im Idealfall analysieren solche Sicherheitslösungen den gesamten bidirektionalen HTML-Datenverkehr, um Angriffe auf Anwendungsebene zu identifizieren und abzuwehren. Auch die SSL-verschlüsselte Kommunikation gilt es zu durchleuchten; denn auch dieser Datenverkehr ist nicht per se geschützt. Oft versuchen Hacker, Attacken über geschützte SSL-Tunnel auszuführen und sie so vor Netzwerk-Sicherheitskomponenten zu verbergen.



Peter Hanke ist Country Manager Austria bei Citrix Systems (www.citrix.at)

Manche Lösungen erkennen korrektes Anwendungsverhalten auch, indem sie den Abgleich mit einer „White List“ vornehmen und ausschließlich erwünschte Zugriffe weiterleiten. Auch empfiehlt es sich, nach außen alle sensiblen Informationen über die Applikationsumgebung zu verbergen - beispielsweise Server-Adressen, Domain-Bezeichnungen oder Angaben über Betriebssysteme. Angreifer könnten andernfalls gezielt nach möglichen Schwachstellen in der IT-Infrastruktur des Unternehmens suchen. So schützen moderne Sicherheitstechnologien Webanwendungen, ohne dabei ein anderes wichtiges Thema aus den Augen zu verlieren: die Performance. Weil rechen- und speicherintensive Aufgaben von den Web-Servern verlagert werden, verbessern sich in manchen Fällen die Antwortzeiten. ❏

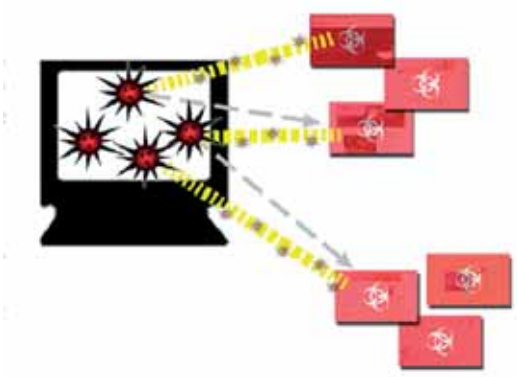
Schutz vor Internet-Bedrohungen

Trend Micro Web Reputation Services durchbrechen die Infektionskette mehrstufiger Internet-Bedrohungen

Internet-Betrüger verwenden heute verschiedene bösartige Aktivitäten und Programme wie Trojaner, Pharming (DNS-Angriffe), Spyware, Adware und viele weitere Malicious Codes. Diese einzelnen Bedrohungen aus dem Internet sind an sich hartnäckig und meist profitorientiert. Die Aussicht auf höhere Profite führt aber zu immer neuen Entwicklungen technisch sehr ausgereifter kombinierter Angriffsmethoden. Sie stellen heute den am schnellsten wachsenden Gefahrenbereich dar.

Diese sogenannten „Blended Threats" zeigen sich in unterschiedlichsten Varianten. Sie bilden eine Kette von Infektionen, die das Internet nutzen, um weitere Exploits und Schadcodes auf Endgeräten einzuschleusen, zu verbreiten und sich auf immer mehr Geräten eines Netzwerks einzunisten. Diese Angriffe können auch durch Hyperlinks in einer Spam-Mail oder ausführbare Dateianhänge ausgelöst werden und sind durch klassische Antiviren Lösungen allein oftmals nicht zu stoppen.

Das mehrstufige Konzept der Trend Micro Web Reputation Services bewertet potenzielle Gefahrenquellen aus dem Internet und schützt vor „Zero-Day-Angriffen", bevor diese Endgeräte und das Netzwerk erreichen können. Die Überprüfung von Abermillionen von Domänen und Webseiten erfolgt anhand von zahlreichen Kriterien wie Verhalten, Historie, Inhaltsanalyse, Standort etc. unter Verwendung von bewährten Techniken und innovativen Trend-Micro-Technologien. Auf diese Weise wird die Vertrauenswürdigkeit von Webseiten vom Hersteller ermittelt und der Anwender kann durch bereitgestellte regelmäßige Updates



und Bewertungen in Echtzeit den Gefahren am Ort ihrer Entstehung begegnen und den Download von Schadkomponenten bereits im Vorfeld verhindern.

PROMOTION

Um mehr zu den innovativen Lösungen von Trend Micro zu erfahren rufen Sie 02236/86 4444-8 an oder schreiben ein Mail an trend_webthreats@3xs-it.com - die ersten Interessenten erhalten Trend Micro PC-cillin Internet Security zum Schutz Ihres PCs gratis!

3xS-it.com

www.3xs-it.com

Symantec präsentiert gesamtheitliches Sicherheitsmanagement

Die Lösung soll die Vorteile verschiedener Sicherheits-Technologien (wie Virenschutz, Antispyware, Desktop-Firewall, Intrusion Prevention und Gerätekontrolle) in einer Single-Agent-Lösung mit zentraler Management-Konsole integrieren.

Symantec Endpoint Protection 11.0 kombiniert Symantec AntiVirus mit erweiterten Abwehrfunktionen und proaktiven Technologien gegen Internetgefahren. Es verbindet integrierte Virenschutz-, Antispyware-, Firewall-, Host- und netzwerkbasierte Intrusion-Prevention-Lösungen (IPS) sowie Applikations- und Gerätekontrolle in einer einzigen Paketlösung. Symantec Endpoint Protection bietet neben der neuen, vereinfachten Konsole auch die Möglichkeit, die Netzwerkzugangskontrolle (Network Access Control, NAC) direkt nach Installation zu aktivieren. Unterstützt werden diese Technologien durch den Zugriff auf das Know-how des Symantec Global Intelligence Network.

Mit Symantec Network Access Control 11.0 steht außerdem ein optionales Modul zur Verfügung, das eng in Symantec Endpoint Protection eingebunden ist. Damit unterstützt es Veranwortliche beim Erkennen und Auswerten des jeweiligen Endgeräte-Status, ermöglicht die erforderlichen Netzwerkzugriffe, stellt Korrekturoptionen bereit und gewährleistet so die Einhaltung geltender Sicherheitsrichtlinien und -standards.

Da sich der Kreis derjenigen, die auf Unternehmensressourcen zugreifen, ständig erweitert, lassen sich der Bedarf an Sicherheitslösungen auf den Endgeräten und die Gewährleistung sämtlicher Sicherheitsrichtlinien nicht länger getrennt betrachten, ist man bei Symantec überzeugt. Symantec Endpoint Protection ist von Beginn an NAC-fähig. Durch Integration der NAC- und Sicherheitsfunktionalität in eine zentrale Endpoint-Agent-Lösung soll eine schnellere und einfachere Implementierung der Zugangskontrollen-Funktionalität durch Symantec Network Access Control ermöglich werden. Gleichzeitig ist es das Ziel, deutliche Rationalisierungseffekte im operativen Bereich zu erzielen, beispielweise einzelne Software- und Richtlinienaktualisierungen, ein einheitliches Reporting sowie einheitliche Lizenzierungs- und Wartungsmaßnahmen.

www.symantec.de

Österreichische Privatbank Euram setzt auf NOD32

Antivirensoftware des Herstellers ESET sorgt bei Euram Workstations und Servern für Sicherheit.

Private Banking ist ein professionelles Geschäft mit langer Tradition in Österreich. Egal ob Privatperson oder institutioneller Investor - Ziel ist immer der langfristige Vermögenserhalt und optimales Wachstum, auch in schwierigen Marktsituationen. So, wie sich die Kunden auf ihren Finanzpartner verlassen, verlässt sich die Euram Bank mit Sitz im Wiener Palais Esterházy bei der IT-Sicherheit auf NOD32: Die Antivirensoftware des Herstellers ESET schützt die Workstations und Server der Privatbank vor digitalen Schädlingen aller Art.

„Die Ansprüche an die IT-Infrastruktur im Bankwesen sind hoch, Sicherheit hat höchste Priorität. In diesem sensiblen Bereich können wir uns einfach keine IT-Ausfälle leisten", betont Keith Lawrence, IT-Verantwortlicher bei der Euram Bank.

Die persönliche Vertrauensbeziehung zu den Kunden und ein Höchstmaß an Vertraulichkeit sind Grundlagen bei der Arbeit der Euram-Banker. Unzureichend geschützte Workstations oder gar ein Ausfall der IT-Infrastruktur hätten gravierende Folgen. Beim Verlust von unternehmensinternen beziehungsweise geschäftskritischen Daten ist nicht nur der finanzielle Schaden enorm, noch schwerer zählt der Vertrauensverlust bestehender oder zukünftiger Kunden.

Geringer Ressourcenverbrauch

„Die Gefährdungen im Netz haben stark zugenommen. Wir haben eine Antivirenlösung gesucht, die technologisch vor allen Bedrohungen schützt und dabei ein gutes Preis-Leistungs-Verhältnis bietet. NOD32 war für uns dabei die Software, die unsere hohen Sicherheitsanforderungen am besten erfüllt hat", erklärt Lawrence.

In einem umfassenden Test wurden die Stärken von NOD32 schnell klar: Die Antivirensoftware aus Bratislava schützt nicht nur vor Angriffen auf das IT-System, sondern arbeitet auch schnell und ressourcenschonend. Ein weiteres Plus waren die Remote Administrator Console zur zentralen Steuerung der Workstations, die raschen Updates der Virensignaturen und die Heuristik, durch die selbst unbekannte Viren erkannt werden. „Beeindruckend waren und sind vor allem die Scan-Geschwindigkeit und der geringe Ressourcenverbrauch der Software", fasst Mark Harre, Senior Technician und Projektverantwortlicher im IT-Team der Euram Bank, die Erfahrungen mit NOD32 zusammen.

Die komplette Umstellung der IT-Infrastruktur auf NOD32 erfolgte bei Live-Betrieb in nur zwei Tagen. Die Implementierung der Software wurde vom IT-Team der Euram Bank selbstständig durchgeführt, alle Applikationen liefen von Beginn an einwandfrei. Heute schützt NOD32 insgesamt 30 Workstations, die auf dem Betriebssystem Microsoft Windows XP laufen, sowie die File- und Microsoft-Exchange-Server des Bankhauses auf Basis von Microsoft Windows Server 2003. Für die Kompatibilität mit unterschiedlichen Systemen sorgt NOD32 selbst: Das Antivirenprogramm ist von Windows 95 bis Windows Vista einsatzfähig.

Seit April 2007 ist die Sicontact Software Vertriebs GmbH exklusiver Vertriebspartner für NOD32 in Österreich. Mit der renommierten Euram Bank vertraut nun der erste österreichische Finanzdienstleister auf das Produkt - für Béla Csiszér, Geschäftsführer von Sicontact, ein wichtiger Schritt auf dem österreichischen Markt. „Wir vertreiben NOD32 erst seit kurzer Zeit in Österreich - das ist nun ein weiterer Beweis, dass in Österreich Wachstumspotenzial für eine schlanke und sichere Antivirensoftware wie NOD32 besteht", gibt sich Csiszér optimistisch.

www.nod32.at
www.eset.at

„Die Ansprüche an die IT-Infrastruktur im Bankwesen sind hoch, Sicherheit hat höchste Priorität." - **Mark Harre** und **Keith Lawrence**, Euram Bank

Über die Euram Bank

Die European American Investment Bank AG (Euram Bank) ist eine unabhängige österreichische Privatbank, die sich zu 100 % im Besitz des Managements und privater Investoren befindet.

Die Bank wurde 1999 in Wien gegründet. Die Euram Bank bietet maßgeschneiderte Lösungen für vermögende inländische und internationale Privatkunden, Family Offices, Familienunternehmen und institutionelle Kunden. Weitere Informationen finden Sie im Internet unter wwww.eurambank.com

WIR SORGEN FÜR SICHERHEIT

Ein Stromausfall oder Schwankungen in der Netzversorgung können zu Systemstörungen, Datenverlusten oder zu noch schlimmeren Schäden führen. Die einfachste und effektivste Möglichkeit diese Störungen zu vermeiden, ist der Einsatz einer USV-Anlage (**U**nterbrechungsfreie **S**trom**v**ersorgung). Wir gewährleisten mit USV-Anlagen von Aros Ihre sichere Stromversorgung. **Weil Systemwissen entscheidet.**

SCHMACHTL

A-1230 Wien, Kolpingstraße 15 Tel.: (01) 6162180-23
Fax: (01) 6162180-99 E-Mail: usv@schmachtl.at
www.schmachtl.at/usv

Gewinnspiel: BitDefender 2008

Mit BitDefender 2008 stellt der Antivirenspezialist BitDefender eine neue Generation von Sicherheitslösungen vor.

Neben Funktionen zum Schutz vor Malware, Spam und Phishing sind alle Lösungen der BitDefender-2008-Produktfamilie mit dem neuen BitDefender-Spiele-Modus ausgestattet. Dieser sorgt für mehr Rechnerleistung und Sicherheit beim Online-Gaming.

BitDefender 2008 schützt nicht nur PCs vor Viren, Spyware, Spam und Co, sondern sichert zudem auch Handys und PDAs vor Malware-Attacken. Die Produktlinie besteht aus den drei Lösungen. BitDefender Antivirus 2008, BitDefender Internet Security 2008 und BitDefender Total Security 2008. Die Einzellösungen sind als Dreierlizenz verfügbar sein.

BitDefender Total Security 2008 verfügt neben allen Schutzfunktionen , Firewall, Spam- und Phishing-Schutz und Kindersicherung auch über:

- Datensicherung - BitDefender erstellt Sicherungskopien wichtiger Dateien auf lokalen Laufwerken und externen Speichermedien.
- PC Tune-up - BitDefender verbessert die Rechenleistung des PCs, indem es nicht mehr benötigte Dateien und Registry-Einträge entfernt.
- Daten-Shredder - mit Hilfe dieser Funktion lassen sich Dateien und Dateifragmente unwiederbringlich löschen.

Systemvoraussetzungen

PC mit Windows Vista, Windows XP (ab Service Pack 2), Windows 2000 (ab Service Pack 4). BitDefender 2008 unterstützt sowohl 64-Bit- wie auch 32-Bit-Systeme. Die Lizenz besteht für drei Installationen inklusive aller Updates und Software-Aktualisierungen ab Installationsdatum für zwölf Monate.

www.bitdefender.de

Gewinnen Sie mit MONITOR ein Paket BitDefender Total Security 2008

Schicken Sie uns eine Postkarte oder eine E-Mail mit dem Kennwort „BITDEFENDER", und mit ein wenig Glück sind Sie unter den Gewinnern.

Einsendeschluss: 19. November 2007 (Poststempel)

Mailadresse: office@monitor.co.at, Postadresse: Monitor, Leberstraße 122, 1110 Wien

(Das Gewinnspiel erfolgt unter Ausschluss des Rechtsweges; Mitarbeiter des Bohmann-Verlages sind von der Teilnahme ausgeschlossen.)

Proaktive Internetsicherheit?

Bedrohungen aus dem Internet nehmen dramatisch zu und sind für Administratoren von Unternehmensnetzwerken inzwischen eine der größten Herausforderungen.

Vital Security Web Appliance NG-5100 von Finjan

Die Produktfamilie Vital Security Web Appliance von Finjan umfasst verschiedene proaktive Internet-Sicherheitslösungen für Unternehmen.

Dank patentierter verhaltensbasierter Technologien soll bereits am Unternehmens-Gateway vor Bedrohungen aus dem Internet wie Spyware, Phishing, Viren, Würmern, Trojanern und sonstigem bösartigem Code geschützt werden.

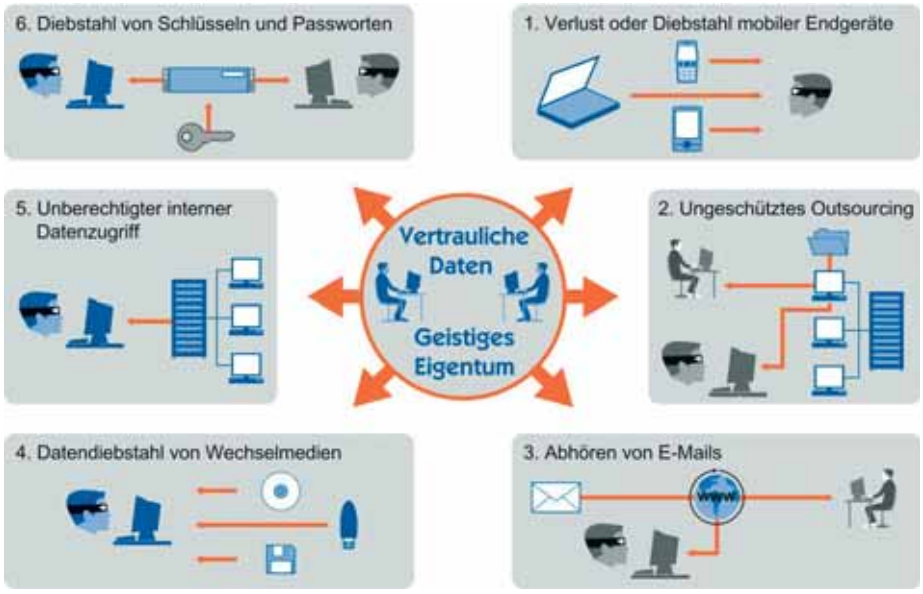
Dazu gehören auch gezielte Angriffe, bösartiger Code auf Cache-Servern, Web-2.0-Angriffe und dynamisch verborgene Codes, die herkömmlicher reaktiver Sicherheitstechnologie verborgen bleiben. Das Security-Modul von Finjan scannt sämtliche Webinhalte. Die Produkte der Vital-Security-Web Appliance-Familie sind in unterschiedlichen leistungsstarken und skalierbaren Varianten erhältlich. Außerdem bieten sie ein zentrales webbasiertes Management, angepasste Protokollierung und Berichterstellung für den Zugriff auf wichtige Betriebsinformationen. Durch Optionen wie einen Load Balancer kann die Verfügbarkeit weiter erhöht werden.

www.finjan.com

Moderne Verschlüsselungsmethoden trotzen den Ressentiments

Datenverlust und -missbrauch zählen zu den folgenschwersten Problemen der IT. Vor allem Anwender mobiler Geräte wie Notebooks oder PDAs gehören zu den Leidtragenden, wenn sensible Informationen in falsche Hände geraten. Einen Ausweg aus dem Dilemma bieten moderne Verschlüsselungsverfahren. Das Problem: Trotz zuverlässiger technischer Chiffriermechanismen herrschen Ressentiments. Zu langsam, zu komplex und zu unsicher, lauten die Vorurteile der Kritiker - zu unrecht.

Olaf Siemens



Allen Unkenrufen zum Trotz hat sich die Verschlüsselungstechnologie in den letzten Jahren zu einem unverzichtbaren Bestandteil für den Schutz sensibler Informationen entwickelt. Dies belegt eine aktuelle Studie des Beratungsunternehmens Experton Group (www.experton-group.de) : Mehr als die Hälfte (51,3%) von 150 befragten Unternehmen in Deutschland nutzen Chiffrierungsmethoden, um ihren E-Mail-Verkehr vor allzu neugierigen Blicken zu schützen. Ruhende - sprich gespeicherte - Daten hingegen, werden lediglich von einem Bruchteil der Auskunftgeber verschlüsselt. Gründe dafür finden sich zum einen in der relativ einfachen Möglichkeit, Verschlüsselungsverfahren für E-Mail-Gateways zu implementieren. Andererseits aber fehlt das Bewusstsein bei vielen Anwendern, dass unternehmenskritische Daten auf Netzwerkspeichergeräten, Festplatten, System- und Netzwerk-Backupgeräten oder aber USB-Geräten der "Bespitzelungsgefahr" ausgesetzt sind. Ebenso gehört die Situation, dass etwa Notebooks aus Unachtsamkeit den Besitzer wechseln könnten, für viele Nutzer oft nicht in die Planung für ein adäquates Sicherheitskonzept. Eine sinnvolle Verschlüsselung kann an unterschiedlichen Punkten im Datenpfad erfolgen - je nach verwendeter Netzwerkarchitektur und entsprechend den geltenden Richtlinien im Unternehmen. Wenn Daten etwa von einem Primärspeicher auf ein anderes Speichergerät verschoben werden, lässt sich eine Verschlüsselung anwenden, ehe die Daten über das Netzwerk verschickt werden - entweder dort, wo die Backup-Anwendung die Daten physisch verarbeitet, oder erst an der Stelle, an der die Backup-Software die Daten in eine Backup-Library oder auf ein langfristiges Speichermedium verschiebt.

Verschlüsselung leicht gemacht

Der entscheidende Punkt jedoch ist immer, die Bewegungen der Informationen und die damit verbundenen Risiken innerhalb des Netzwerks gänzlich zu verstehen. Können Unternehmen Bereiche identifizieren, in denen aktuelle Geschäftsprozesse den Verlust, Diebstahl oder die unbeabsichtigte Offenlegung vertraulicher Informationen hervorrufen können, lässt sich anhand dessen eine umfassende Datensicherheitsstrategie erstellen: Es werden die Stellen im Unternehmen definiert, deren Datenpfad entsprechend gesetzlicher Vorgaben verschlüsselt sein soll. Dies kann Informationen auf Desktops, Notebooks oder gar Flash-Speichermedien der Außendienstmitarbeiter ebenso betreffen, wie wenn Daten an ein Backupgerät im Netzwerk geschickt werden sollen. Der Fokus liegt dabei stets auf einem akzeptablen Kompromiss zwischen erforderlicher Sicherheit und Benutzerfreundlichkeit der einzusetzenden Verschlüsselungslösung.

Ist die Verschlüsselungstechnologie Bestandteil einer Be-

triebssystemarchitektur oder einer Open-Source-Lösung ist der Einsatz heute relativ leicht, andererseits aber nur bedingt flexibel und umfassend. Zusätzliche Verschlüsselungstools bieten sich für Unternehmen an, die nach End-to-End-Lösungen streben, um die Vertraulichkeit von Daten und den Schutz der Unternehmenskommunikation sicherzustellen, und die eine präzise Kontrolle über unterschiedliche Sicherheitsaspekte benötigen.
Denn: Den betriebssystembasierten Schutzfunktionen mangelt es zumeist an einer zentralen Administration sowie an einer kontrollierten Sicherung der verwendeten Verschlüsselungsschlüssel. Bordmittel reichen auch dann oft nicht mehr aus, wenn Unternehmen verschiedene Betriebssysteme im Einsatz haben: Sie können nicht übergreifend verschlüsseln und verfügen kaum über Berichts- und Protokollfunktionen. Dies ist vor allem zur Einhaltung gesetzlicher Bestimmungen dringend erforderlich.

Herrschaft über die Verschlüsselungsprozesse

Spätestens mit zentralen und vereinfachten Kontroll- und Administrations-Möglichkeiten für die Chiffrierung lassen jüngste Produkte den Vorwurf der Komplexität hinter sich: Diese neue Security-Strategie erfordert zwar mehr Planung als die herkömmliche Verschlüsselung von reinen "Endpunktgeräten" wie Notebooks, doch der Mehraufwand hilft, die laufende Wartung der Lösung zu optimieren. Zentral verwaltete Datensicherheitsprodukte sorgen außerdem für eine erhöhte Konsistenz der Systemaktivitäten, indem sie die Benutzer beispielsweise davon abhalten, Änderungen an der Betriebssystemkonfiguration vorzunehmen. So verringert sich auch der Aufwand für die IT-Administration.

Der Vorteil: Einstellungen lassen sich einfach in einer Konfigurationsdatei vornehmen und die Software von einem zentralen Ort aus im gesamten Unternehmen bereitstellen - je nachdem, welche Mechanismen - ob Microsoft Active Directory oder System Management Server (SMS) - greifen. Dieser Komfort spiegelt sich auch darin wider, dass die Belegschaft keine Schulung benötigt. Nach der Installation erhalten Mitarbeiter einen neuen Anmeldebildschirm, sobald sie ihren Computer starten, mehr nicht. Sämtliche Ver- und Entschlüsselung aller oder ausgewählter Dateien erfolgt im Hintergrund, und hat keine merklichen Auswirkungen auf die Produktivität der Anwender.

Erweiterung auf digitale Speicherzwerge

Besonders gefährdet sind indes Daten auf Kleinstgeräten wie externe Festplatten, Flash-Karten, USB-Sticks oder optische Medien. Unternehmen sollten daher neben E-Mail- und File&Folder-Verschlüsselung ihre Datensicherheitsstrategie auch darauf ausweiten, um dem Risiko des Verlusts oder Diebstahls gespeicherter Daten zu begegnen. Ein durchdachtes Anwendungsdesign moderner Verschlüsselungen nutzt geringe Prozessorauslastungen dazu, um Ver- und Entschlüsselungsaufgaben on the fly zu erledigen.

Leistungsknick passé

Performance-Aspekte lassen sich dank schneller Verschlüsselungsalgorithmen demnach fast völlig vernachlässigen. Die einzelnen Verschlüsselungsprodukte unterscheiden sich jedoch in ihrer Effizienz und in den allgemeinen Auswirkungen auf die Performance. Es ist schwierig, die Performance zwischen unterschiedlichen Plattformen, Systemen und Anwendungen zu vergleichen. Doch unabhängige Organisationen erstellen gelegentlich Vergleiche zwischen ähnlichen Produkten für bestimmte Marktsegmente und können Aufschluss über mögliche Auswirkungen der Chiffrierung auf den Geschäftsbetrieb geben. Als grobe Richtlinie gilt, dass herkömmliche Verschlüsselungsprodukte bei normaler Nutzung die Performance um etwa 6-8% verringern - neueste Datensicherheitslösungen dagegen nur um 2-5%. Eine solch marginale Leistungseinbuße wird von Anwendern in der Regel jedoch nicht wahrgenommen.

Schlüssel in den Hochsicherheitssafe

Ein Risiko stellt allerdings der Diebstahl kryptografischer Schlüssel dar. Besonders der Master-Key verlangt nach besonderen Schutzvorkehrungen - von ihm sind alle weiter eingesetzten Schlüssel des Unternehmens abgeleitet. Die derzeit zuverlässigste Lösung ist die hochsichere Speicherung der Schlüssel in einem Hardware-Sicherheitsmodul (HSM). Im Gegensatz zur Softwarebasierten Lösungen sind HSM manipulationssicher und sorgen für eine sichere Generierung, Speicherung und Anwendung von kryptografischen Schlüsseln und Zertifikaten bei Verschlüsselungs- und Signaturverfahren.

Olaf Siemens ist Entwicklungsleiter beim Security-Spezialisten Utimaco

Die Qual der Wahl

Jedes Unternehmen muss letztlich für sich entscheiden, wie das Gleichgewicht zwischen einer offenen Kommunikation zwischen Geschäftspartnern, Klienten, Lieferanten, Kunden und Mitarbeitern einerseits und dem notwendigen Grad an Datensicherheit andererseits erreicht werden kann, um die entsprechenden gesetzlichen Vorgaben zu erfüllen und Datenschutzrichtlinien zu entsprechen.

Alle Verschlüsselungsprodukte sind unterschiedlich: Während Freeware-Lösungen für viele Privatanwender attraktiv sind, erfüllen sie nur in den seltensten Fällen die Anforderungen von Unternehmen, da ihnen zumeist die nötigen Features und Managementfähigkeiten fehlen. Einzellösungen, wie sie Verschlüsselungsprodukte für bestimmte Geräte darstellen, sind zumeist nicht in der Lage, sämtliche Sicherheitsrisiken zu beachten, die in Netzwerkinfrastrukturen und bei mobilen Mitarbeitern auftreten können. Unternehmen mit hohen Sicherheits- und Effizienzansprüchen sollten sich daher nach Lösungen umsehen, die speziell für den Unternehmenseinsatz konzipiert wurden und Fragen der gesetzlichen Rahmenbedingungen, Arbeitsprozesse mit offenen Infrastrukturen, zunehmende Mobilität der Mitarbeiter sowie ausgeweitete E-Commerce-Aktivitäten abdecken können. Denn: Der Verlust von geschäftskritischen Informationen ist es nicht wert, an der falschen Stelle zu sparen. ❑

„Mobility Award 2007“ für mobilkom austria und mobildata

Im Rahmen der Businessworld Awards wurden mobilkom austria und mobil-data mit dem „Mobility Award 2007“ ausgezeichnet.

Der Preis geht an das Produkt „md-sales“ - eine Lösung für verschiedenste Vertriebsanwendungen von Logistik über Fahrverkauf bis hin zu CRM. mobilkom austria hat bereits zum zweiten Mal in Folge diesen Award gemeinsam mit einem A1-Solution Partner erhalten. Verliehen wurde die Auszeichnung im Rahmen der Businessworld Awards für besondere wirtschaftliche Leistungen von der Wirtschaftskammer Wien und dem Businessworld Magazin.

Ausschlaggebend für die Entscheidung waren neben den wirtschaftlichen Erfolgen auch Kreativität, Zukunftsorientierung und ein sympathischer Markenauftritt. DI (FH) Haimo Lorenz, Partner Manager mobilkom austria und Ing. Thomas Gruber, Geschäftsführer von mobil-data, nahmen den „Mobility Award 2007“ gemeinsam entgegen.

Bei dem Produkt, das als mobile Lösung des Jahres ausgezeichnet wurde, handelt es sich um md-sales, die mobile Fahrverkaufslösung für Santora Kaffee Systeme GmbH. mobil-data GmbH hat die bestehende Softwarelösung um eine mobile Push Technologie, md-Heartbeat, erweitert. Dadurch kann Santora die Touren- und Einsatzplanung optimieren und damit seine Logistikprozesse effizienter und kostengünstiger gestalten.

„Der Mobility Award, den wir bereits zum zweiten Mal in Folge erhalten haben, ist nicht nur eine Bestätigung für den Erfolg des Programms, sondern auch dafür, dass wir zukünftig mit unseren Partnern noch intensiver zusammenarbeiten werden“, so Dr. Hannes Ametsreiter, Vorstand Marketing, Vertrieb und Customer Services, mobilkom austria und Marketingvorstand Telekom Austria TA.

(V.l.n.r.): DI (FH) **Haimo Lorenz** (Partner Manager mobilkom austria), **Klaus Risser** (Key Account Manager mobilkom austria), Gen.Dir. **Joost Wetzels** (Geschäftsführung Santora Kaffee GmbH), **Stephan Hüttner**(Mobile Consultant mobil-data IT & Kommunikationslösung GmbH), **Peter Lieber** (COO mobil-data IT & Kommunikationslösung GmbH), **Thomas Gruber** (Geschäftsführung, COO mobil-data IT & Kommunikationslösung GmbH)

Faszniert

davon, dass Erfolg weitere Erfolge anzieht? Ein guter Grund, sich jetzt für eine preisgekrönte Unified Communications Lösung zu entscheiden. Wie den SIP-Softswitch HiPath 8000 – perfekt für große oder dezentralisierte Unternehmen. Mit dem Know-how und der Sicherheit, die Sie von einem Frost & Sullivan EMEA Award Winner für Unternehmenstelefonie erwarten können. Open Communications von Siemens Enterprise Communications. Effiziente Lösungen für optimierte Geschäftsprozesse.

Communication for the open minded

Siemens Enterprise Communications: www.siemens.at/open

SIEMENS

Komplexität der IT beschert IT-Beratern Hochkonjunktur

Nach der Krise 2002/2003 ist der IT-Berater-Markt in Österreich wieder gut erholt. Immer raschere Produktzyklen, der Innovationsdruck sowie die Komplexität der hausinternen IT-Architektur und Applikationen verhelfen den IT-Beratern zu vollen Auftragsbüchern. Grund genug für MONITOR-Chefredakteur Rüdiger Maier, Mitte Oktober eine Expertenrunde zum Thema „Aktuelle Trends und Herausforderungen in der IT-Beratung" zu versammeln.

Christine Wahlmüller

Immer mehr Unternehmen erkennen, dass mit einer optimierten Informationstechnologie die Geschäftsprozesse besser laufen, was sich wiederum „gut für´s G´schäft" erweist. Damit die IT „rund" läuft, werden gerne IT-Berater zu Hilfe geholt. Dabei wird jedoch auf eine Grundvoraussetzung meist vergessen, die helfen könnte, viel Geld zu sparen: das beidseitige Verständnis - einerseits von Management, Marketing und Vertrieb sowie den Fachabteilungen und andererseits von der hausinternen IT-Abteilung und eventuellen externen IT-Mitarbeitern und Beratern.

„Man muss auch die Leute in die Pflicht nehmen, die die Konzepte machen." - **Wilfried Seyruck**, WKO

Viele Manager haben keine Lust oder Zeit, sich mit der Technik auseinanderzusetzen, sondern haben vor allem Produktion, Marketing, Vertrieb und Umsatz im Auge. Die EDV ist oft ungeliebter und unverstandener Teil des eigenen Hauses. Kein Wunder, dass laut einer A.T.Kearney-Studie, bei der 65 Top-Manager aus Österreich und Deutschland befragt wurden, genau diese Führungsriege urteilte, dass die unternehmenseigene IT den Geschäftsanforderungen nur unzureichend entspricht. Die hauseigene IT wird als Wachstumsbremser gesehen und erlebt und beschert nach Meinung der Manager den Unternehmen durchschnittlich 5% weniger Umsatzwachstum.

Nur: Wer von den befragten Herrschaften nimmt sich tatsächlich die Zeit, die hauseigene IT zu verstehen, mit der IT-Abteilung konstruktiv zusammenzuarbeiten oder die eigenen Anforderungen so auf den Tisch zu legen, dass sie von der IT-Abteilung auch adäquat umgesetzt werden können? Ein gern benützter Ausweg aus dem internen Dilemma bieten externe IT-Berater. „Viele Firmen wissen zu wenig, was sie mit IT tun können oder wie sie ihr Geschäft mit IT unterstützen können", eröffnete Rüdiger Maier, Chefredakteur des MONITOR, die Gesprächsrunde. Genau hier könnten IT-Berater ja gut ansetzen. Für größere Betriebe sind externe Berater heute beinahe schon selbstverständlich. Wie sehen nun die Erfahrungen aus der Praxis der Berater aus?

„Alle großen Hersteller haben heute eine Suite, die nicht zusammenpasst." - **Siegmund Priglinger**, BARC

IT-Alltag bei der NÖM

Um nicht nur theoretisch zu diskutieren, war auch ein IT-Leiter, Anton Leitner von der NÖM AG, zur Runde geladen, um aus der Praxis der IT und der Zusammenarbeit mit IT-Beratern zu berichten. Leitner, früher selbst IT-Berater bei Capgemini, und Spezialist für die Einführung von SAP, kennt beide Seiten: „Früher, noch vor zehn Jahren waren wir die Götter, und in den Unternehmen gab es wenig Wissen über SAP. Heute, vor allem nach dem Crash der Branche 2002, hat sich das Bild sehr gewandelt."

Von Beratern werde heute mehr erwartet, und intern sei das Wissen deutlich größer, urteilte der NÖM-IT-Leiter. Zur Zeit ist Leitner selbst für die SAP-Einführung seines Unternehmens verantwortlich, ein Riesen-Projekt, das in Zusammenarbeit mit einem Siemens-Tochterunternehmen, der

unit-it, 2008 realisiert werden soll.

Heute wird Beratung seiner Meinung nach aus drei Gründen verwendet:

- Man hat intern zu wenig Ressourcen.
- Man ist zu feige und will Verantwortung abwälzen.
- Man kauft Wissen zu.

In den USA werde IT-Beratung vielfach auch als Statussymbol betrachtet, ergänzte Leitner.

„Herstellerunabhängigkeit sehe ich als wichtiges Thema der Zukunft." - **Michael Bauer**, Trivadis

„Den Berater als Ausrede zu verwenden - das ist stark zurückgegangen", stellte Josef Matulka, Mitglied der Geschäftsleitung bei Capgemini, fest. Der Berater werde eher dazu verwendet, einen Weg aus einer unangenehmen Situation zu finden. „Der Kunde heute schaut schon, dass er das Projekt in der Hand hat", stellte Ewald Halbedl, Geschäftsführer von VMCP (Vienna Management Consulting Partner), fest. „Der Berater muss auf das Gesamtsystem schauen und er muss dessen Funktionieren gewährleisten", betonte Johannes Adler, Geschäftsführer und Gründer von Anecon. Er verglich den Berater mit einem Arzt. „In der chinesischen Medizin wird der Arzt gezahlt, wenn der Patient gesund ist - das entspricht dem Berater eher als unsere Ärzte, die erst auf Krankheitssymptome reagieren."

„Der Kunde erwartet allerdings, dass man nicht nur ein Konzept abgibt." - **Ewald Halbedl**, VMCP

Schwierige Rolle des IT-Beraters

In der Folge wurde über die Planung und Realisierung von IT-Projekten diskutiert. „Im öffentlichen Bereich ist es ohnehin so: Es gibt eine strikte Trennung zwischen Planung und Erbringungsleistung", erläuterte Adler. „Der Kunde erwartet allerdings, dass man nicht nur ein Konzept abgibt", wies Ewald Halbedl darauf hin, dass in der Praxis sehr wohl Planung und Realisierung gemeinsam erwünscht sei. „In der IT-Beratung kann man es sicher nicht trennen. Man muss auch die Leute in die Pflicht nehmen, die die Konzepte machen", meinte Wilfried Seyruck, einerseits Obmann-Stellvertreter des Fachverbands Unternehmensberater und Informationstechnologie (UBIT) sowie Geschäftsführer der Linzer „Programmierfabrik." „Viele Unternehmen sind erwachsener geworden und kaufen heute gezielt punktuell zu, was sie brauchen", so Seyruck. Open Source sei eine komplexe Welt geworden. „Wir brauchen da sogenannte Hybrid-Menschen. Einerseits sollen sie ein sehr weitreichendes IT-Wissen haben, andererseits sich mit dem jeweiligen Business des Kunden auskennen", stellte Seyruck die schwierige Anforderung für optimale IT-Beratung in den Raum.

„Über 90% der Berater haben einen ‚Produktstempel' am Rücken." - **Peter Schneyder**, PanPlan

„Über 90% der Berater haben einen Produktstempel am Rücken, es gibt die Trennung nicht im Angebot", erläuterte Peter Schneyder, Geschäftsführer von PanPlan, der überdies ein anschauliches Beispiel parat hatte. „Wenn jemand ein Kochrezept ausprobiert, und das Essen schmeckt dann nicht gut, würde es niemandem einfallen, den Herdhersteller zu fragen, warum es nicht funktioniert hat.

Aber im IT-Bereich arbeiten wir genau so." IT-Anwender würden SW- und HW-Herstellern Fragen über Fragen stellen. Schneyders Appell: „Die Hersteller sollten sich mit dem Anwender und seiner Logik mehr auseinandersetzen."

Eine der großen Herausforderungen, darin waren sich die Teilnehmer einig, liegt sicher in der zunehmenden Komplexität der IT. „Alle großen Hersteller haben heute eine Suite, die nicht zusammenpasst", stellte Siegmund Priglinger, Repräsentant von BARC (Business Applications Research Austria) fest. „Wir von BARC haben SW-Labs, da sehen wir, wie die Dinge zusammenpassen", verwies Priglinger auf praxisorientiertes Know-how. „Wir sehen, dass die klassische Unternehmensberatung mit der IT zusammenwächst", gab Wilfried Seyruck einen weiteren Punkt zu bedenken. Anders gesagt: Es gibt einen immer engeren Zusammenhang zwischen IT und Geschäftsentwicklung.

„SAP war ein Glücksfall für Europa." – **Georg Lankmayr**, INSET

Rückhalt durch Wissenschaft

„Inwieweit ist die Anbindung an die Wissenschaft oder Universität, die testen kann, eine Voraussetzung, um als Berater neutral sein zu können?", wollte Moderator Maier wissen. „Die Erkenntnisse aus der Praxis sind zum Teil weit vor dem, was die Wissenschaft nachvollziehen kann", gab Siegmund Priglinger eindeutig den Praktikern den Vorzug.

Dem widersprach Anecon-Geschäftsführer Johannes Adler: „Ein ständiger Dialog mit der Wissenschaft ist sicher wichtig." „Aber wir haben leider wenige aus der österreichischen Professorenschaft, die einen echten Praxisbezug haben", bedauerte Priglinger. „Wir arbeiten schon mit Universitäten zusammen, aber die großen Mega-Impulse kommen nicht von dort, die großen Strategie-Portfolio-Modelle wurden dort nicht entwickelt, sondern die kommen aus der Berater-Praxis", betonte Josef Matulka, der die Aufgabe der Universität eher in der Reflexion und in sozialwissenschaftlichen Querschnitt-Studien sieht.

Eine Erfahrung der anderen Art machte Georg Lankmayr, TU-Absolvent und Geschäftsführer von Inset, spezialisiert auf Telekommunikationsberatung: „Gehen Sie nach Hause mit ihren Beraterfolien", sagte ein Uni-Professor zu Lankmayr, der vor seiner Dissertation bereits als IT-Berater tätig gewesen war. Das Verhältnis Berater - Uni scheint also keineswegs ein optimales zu sein. „In Österreich gibt es leider keine

„Am Ende schaut bei ERP-Projekten meist SAP heraus." - **Joachim Seidler**, IDC

Picaults und Scheers", bedauerte Lankmayr. „Es liegt sicher noch enormes Potenzial brach, das viel mehr genutzt werden könnte und in Österreich viel zu wenig gefördert wird", kritisierte Lankmayr. Dazu passt eine soeben präsentierte Studie, des Fraunhofer Instituts, die u. a. zum Ergebnis kam, dass die österreichische Forschung auf keinem IKT-Gebiet international vorne mit dabei ist.

Wertschätzung für IT steigt

Zurück zum Thema lenkte Keith Stammers, Consultant bei Softlab. Sehr oft würden IT-Projekte gemacht und erst danach werde über Auswirkungen nachgedacht. So soll es natürlich nicht sein. „Ein Trend, den ich erkenne ist, dass man weggeht von der Ansicht, IT als Kostenfaktor zu betrachten. Sondern man reflektiert: Wie viel wert ist meine IT und was möchte ich damit erreichen? Die Rolle des IT-Beraters ist es, die Unternehmen bei der organisatorischen Veränderung einfach zu begleiten", meinte Stammers.

Angesprochen wurde einmal mehr die Schwierigkeit der Kluft zwischen Management und IT, die auch einen Trend auslöst: „Das größte Geschäft machen wir zurzeit im BI-Bereich (Business Intelligence), die Neueinführung von Systemen ist immer gekoppelt mit Kompetenzzentren", stellte Siegmund Priglinger klar. BI wird heute auch operativ, nicht mehr nur strategisch eingesetzt. „Das Management, das null Ahnung von IT hat, entscheidet leider oft blind für irgendeine IT-Lösung", bedauerte Peter Schneyder. Ewald Halbedl hakte ein: „Genau da sehe ich meine Rolle als Berater, dass ich frage: Was sind Deine Prozesse und was möchtest Du erreichen? Und wenn ich den Eindruck habe, dass das keineswegs klar ist, dann werde ich sagen: Du brauchst vorher ein anderes Projekt, bevor du über ein neues IT-System nachdenkst."

Wichtig sei der Begriff der „Agilität", betonte Josef Matulka, darüber habe man vor kurzem bei Capgemini eine Studie gemacht, wobei CIOs empirisch befragt wurden. Ein wesentlicher Hinderungsgrund, der dabei entdeckt wurde, sei die Erkenntnis, dass Agilität und Flexibilität auch in die Menschen der IT-Abteilung „hineinmüsse". Zum gleichen Begriff passend hatte auch Georg Lankmayr eine eigene Studie, durchgeführt bei Mobilfunkanbietern, parat. Dabei wurde gefragt, wer wohl die Treiber bzw. „Verhinderer" bei Veränderungen der IT seien. Die Erkenntnis: Meist sind die IT-Leiter die größten Bremser für Mobility-Themen, mit altbekannten Argumenten wie z. B. Security. Damit kam das Gespräch wieder auf die mangelnde Kommunikation und das Missverständnis zwischen Management, Fachabteilung und hausinterner IT zurück.

„Den Berater als Ausrede zu verwenden, das ist stark zurückgegangen." - **Josef Matulka**, Capgemini

„Die Rolle des IT-Beraters ist es, die Unternehmen bei der organisatorischen Veränderung einfach zu begleiten." - **Keith Stammers**, Softlab

„Die Aufgabe des Beraters ist es sicher, da ein Bindeglied zu sein und diese zwei Welten zueinander zu bringen", brachte es Michael Bauer, Niederlassungsleiter von trivadis, auf den Punkt. Die Frage ist, wie die IT-Beratung auf dieses bekannte Problem reagiert. „Daraus resultiert eine Spaltung der IT-Beratung. Es gibt die IT-Beratung, die eigentlich eine spezialisierte Unternehmensberatung ist. Ein gutes, großes strategisches IT-Projekt ist ja eigentlich ein Business-Projekt, eine CRM-Initiative, eine Supply-Chain-Initiative. Das hat wenig zu tun mit der konkreten Implementierung eines Systems", erklärte Josef Matulka. „Also die IT-Berater mit dem Bauchladen gibt es einfach nicht mehr. Die Branche hat sich fokussiert. Der nächste Schritt ist es, Partnerschaften zu bilden, und die Bereitschaft zusammen zu arbeiten, wird auch immer größer", betonte Wilfried Seyruck vom UBIT (WKO, Fachverband für Unternehmensberatung und Informationstechnologie). Der Verband hat 40.000 Mitglieder, 28.000 davon sind IT-Unternehmen. Der Frauenanteil liegt bei knapp 10% und 60% sind Ein-Person-Unternehmen.

Auslands-Ambitionen und Kritik

Ein Trend zeigt auch in Richtung Internationalisierung und Ausdehnung. Viele Berater begleiten ihre Kunden bei der Expansion ins Ausland. „Jeder Beratungs-Euro im Ausland hat einen Riesen-Multiplikationseffekt", freute sich UBIT-Vertreter Seyruck. „Kleinere Berater haben aber mit der Expansion schon Probleme", gab Ewald Halbedl zu bedenken. Größere Berater können es sich leisten „Tochterfirmen im Ausland bzw. in Osteuropa gründen", sagte

Teilnehmer (alphabetisch):

Dr. **Johannes Adler**, Geschäftsführer ANECON
Michael Bauer, Geschäftsführer Trivadis Österreich
Dipl.Ing. Mag. **Ewald Halbedl**, GF von VMCP (Vienna Management Consulting Partner)
Dipl.Ing. **Georg Lankmayr**, Geschäftsführer INSET
Dipl.Ing. **Anton Leitner**, IT-Leiter NÖM
Dr. **Josef Matulka**, Mitglied der Geschäftsleitung Capgemini Österreich & Eastern Europe
Dr. **Siegmund Priglinger**, BARC Österreich
Peter Schneyder, Geschäftsführer PanPlan
Dipl.Ing. **Wilfried Seyruck**, WKO, Obmann-Stv. UBIT
Joachim Seidler, Niederlassungsleiter IDC Österreich
Keith Stammers, Softlab, Prokurist und Senior Consultant
Moderation: Dipl.Ing. **Rüdiger Maier**, Chefredakteur MONITOR
MONITOR-Autorin: Dr. **Christine Wahlmüller-Schiller**
Fotograf: **Andreas Partusch**
Ort der Diskussion: Capgemini Consulting, 1020 Wien

Josef Matulka von Capgemini. Wien ist als Tor nach Osteuropa sehr beliebt. Auch Capgemini hat sein Osteuropa-Headquarter in Wien.

Eine neue Perspektive steuerte Joachim Seidler, Österreich-Geschäftsführer des Markforschungsunternehmens IDC, bei: Die Frage sei, wie User die Berater sehen würden. „Ich sehe da vor allem einmal das Problem der Verantwortlichkeit, aber auch die mangelnde Unabhängigkeit der Berater", so Seidler. „Am Ende schaut bei ERP-Projekten meist SAP heraus." Leider sei die Beratung oft zum Scheitern verurteilt, „weil es für viele Unternehmen schwierig ist, zu erkennen, wie die IT optimal zur Unterstützung der Geschäftsprozesse eingesetzt werden kann." In der Beratungsbranche, prognostizierte Seidler, werde es künftig „weiter große Wachstumsraten" geben.

Weiterer Aspekt: Auch viele Systemhäuser und IT-Hersteller wollen beim IT-Beratungsgeschäft mitmischen und bezeichnen sich selbst gerne als Berater. Die Konkurrenz am Markt ist groß. Insgesamt droht der Branche in Zukunft ein echter Fachkräfte-Mangel. „Leider ist IT auch noch immer eine Männer-Domäne", bedauerte Seyruck. Frauen hätten da gute Chancen.

„Der Berater muss auf das Gesamtsystem schauen und er muss dessen Funktionieren gewährleisten." - **Johannes Adler**, ANECON

Trends und Wünsche

„Wir produzieren viel zu wenig SW-Produkte, das ist ein wesentlicher Mangel in Österreich", stellte Siegmund Priglinger fest. „Wenn es uns nicht gelingt, SW-Produkte auf den Markt zu bringen, werden wir mit der Dienstleistung auch in Zukunft ein Problem haben", so Priglinger. „SAP war ein Glücksfall für Europa. Ich würde mir wünschen, dass wir ein zweites, drittes oder viertes SAP bekommen", schloss sich Georg Lankmayr an.

„Ich wünsche mir eine bessere Kommunikation zwischen IT und Management", meinte Keith Stammers kurz und bündig. „BI und Datawarehouse sind die wichtigsten Themen. Herstellerunabhängigkeit sehe ich als wichtiges Thema der Zukunft", sagte Michael Bauer. „Eine gute IT-Beratung muss sich in der Umsetzung beweisen. Den Kunden interessiert nicht allein das Konzept, sondern der Beweis, dass es funktioniert", meinte Josef Matulka.

Wichtig ist sicher das „Verständnis des Beraters, eine Wissensorganisation zu sein", betonte Johannes Adler. „Ein guter Berater muss ein guter Kommunikator und Netzwerker sein, im besten Fall jemand, der nicht aus der IT kommt, aber IT versteht", formulierte IDC-Marktforscher Joachim Seidler. „IT sollte als value Lieferant gesehen werden, nicht als notwendiges Übel", so die Empfehlung von Ewald Halbedl. „Die Zahl der Berater wird sich weiter vergrößern und Spezialisierungen werden noch zunehmen", prognostizierte UBIT-Branchenvertreter Wilfried Seyruck rosige Zeiten für die IT-Berater. „Die NÖM wird 2008 ein großer Konsument von IT-Beratung sein", sorgte NÖM-IT-Leiter Anton Leitner für den passenden Schlusspunkt. ❑

(Alle Bilder: Andreas Partusch/ Fotofc)

Was

haben Frisch-Fracht-Speditionen

und Mineralölkonzerne

gemeinsam?

Beide Unternehmen entwickeln, erweitern und integrieren ihre Anwendungen mit der innovativen Technologie von InterSystems. Als weltweit erfolgreiches Softwareunternehmen mit mehr als 28 Jahren Erfahrung unterstützen wir auch Sie dabei, wenn es darum geht, Zeit und Geld zu sparen! Entdecken Sie jetzt das Erfolgsgeheimnis führender Unternehmen aller Branchen und **Innovationen** von **InterSystems**

Machen auch Sie
Ihre Anwendungen erfolgreicher:
www.InterSystems.de/Erfolg

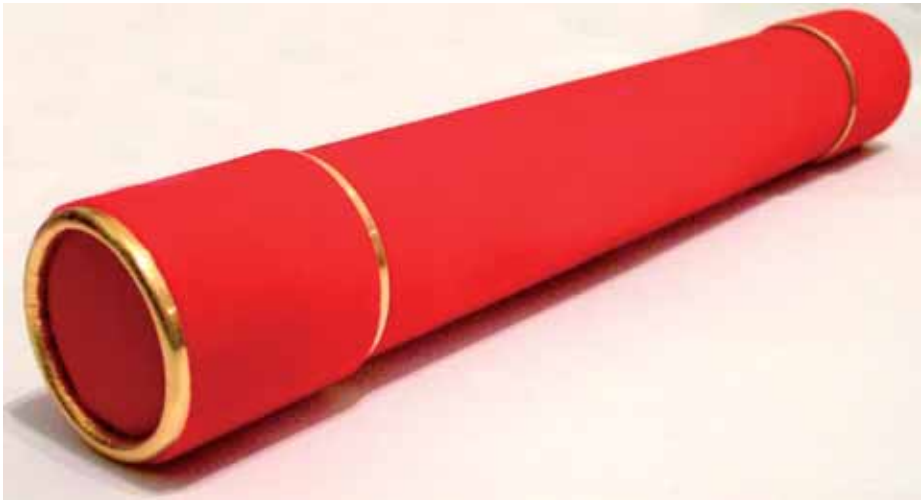
InterSystems

InterSystems GmbH · Hilpertstr. 20a · D-64295 Darmstadt
Telefon +49.6151.1747-0 · Fax +49.6151.1747-11

Praxisorientiert und schnell zu Wissen und Titel

Das Ausbildungsangebot im Bereich Informationstechnologie (IT) oder Telekommunikation (TK) ist vielfältig wie noch nie. Waren im ersten Teil der MONITOR-Serie (Heft 9) die österreichischen Universitäten an der Reihe, so berichten wir im zweiten Teil über alle IT/TK-Studiengänge der Fachhochschulen in Wien, Niederösterreich, Burgenland und in der Steiermark.

Christine Wahlmüller



Die Fachhochschulen (FH) blicken auf eine erst junge Geschichte zurück. Zehn FH-Studiengänge waren es, die im Studienjahr 1994/95 den Studienbetrieb aufnahmen. Heute gibt es 195 (!) FH-Studiengänge in Österreich und knapp 30.000 Studenten an den österreichischen Fachhochschulen. Aus dem einst von den Unis eher belächelten Praktikerschmieden sind ernstzunehmende Konkurrenten im Bildungssektor geworden.

„Wir bieten Spezialisierungen wie Technische Informatik und Geoinformatik an." - **Martin Staudinger**, FH Wiener Neustadt, Studiengangsleiter Informationstechnik

Drei Viertel aller Studiengänge sind heute schon auf das neue Studiensystem (Bachelor-Master) umgestellt, im kommenden Jahr sollen es 90% sein. Noch eine interessante Zahl: Die FH bietet auch Berufstätigen eine gute Weiterbildungsmöglichkeit. 40% der Studiengänge werden berufsbegleitend angeboten. Die meisten FH-Studenten finden sich in Wien (7.517), gefolgt von NÖ (4.181), Steiermark (3.782) und OÖ (3.742). Alle Zahlen vom vergangenen Studienjahr 2006/07. Die Zahl der technischen und IT-TK-Studiengänge nimmt ständig zu bzw. ist ein echter Trend in Richtung Spezialisierungen (vor allem beim Masterstudium) zu bemerken.

Neu: Wirtschaftsinformatik neben dem Job

Mit etwa 1.700 AbsolventInnen und knapp 2.200 Studierenden sowie derzeit elf Bachelor- und 14 Master-Studiengängen ist die Fachhochschule Technikum Wien der größte Fachhochschul-Anbieter für technische Studien in Österreich. In puncto IT- und Telekommunikation werden fünf Bachelor- und fünf Master-Studiengänge angeboten. (Alle Studienorte und Studiengänge siehe Kasten.) Ab dem kommenden Wintersemester kann zusätzlich noch das neue Master-Studium „Game Engineering und Simulation" belegt werden.

Heuer gibt es erstmals die Möglichkeit, Wirtschaftsinformatik auch berufsbegleitend am Technikum zu studieren. „Das bedeutet an drei Tagen in der Woche jeweils vier Stunden Unterricht", erläutert Studiengangsleiter Helmut Gollner. Im Unterschied zur Uni geht es bei der FH „um Lernen mit kleinen Gruppen und einen sehr starken Praxisbezug", betont Gollner. Das Technikum unterhält zahlreiche Kooperationen mit IT-Betrieben wie IBM, Microsoft, Unisys oder Accenture. „In jedem Semester wird auch ein praxisnahes Studentenprojekt durchgeführt, z. B. ein Webshop für eine Firma. „Das Wirtschaftsinformatik-Studium sorgt für eine gesamtheitliche Sicht auf IT-Lösungen", erklärt Gollner die Vorzüge des Studium. Neben der Technik werden auch Faktoren wie Finanzierbarkeit, Menschen, Organisation oder Wissen um die Einführung von Systemen vermittelt. Gut für die Studenten sind auch die vielen externen Lektoren aus der Praxis (80%), die ein lebendiges und anschauliches Bild aus der IT-Praxis zeichnen. Insgesamt sind etwa 1.220 Studenten in den IT-TK-Studien angemeldet, d. h. in etwa jeder zweite Student studiert IT.

„Im Unterschied zur Uni geht es bei der FH um Lernen mit kleinen Gruppen und einen sehr starken Praxisbezug." - **Helmut Gollner**, FH Technikum Wien, Fachbereichsleiter Wirtschaftsinformatik

Nur noch Bachelor-Master-Titel

Zweitgrößter Wiener Anbieter ist die FH Campus Wien, die erst im Sommer 2004 den Status Fachhochschule verliehen bekommen hat. Sie hat alle Studiengänge ab dem heurigen Wintersemester auf das neue Bachelor-/Master-System umgestellt. Zurzeit gibt es drei Bachelor-Studiengänge. Drei Master-Studiengänge („IT-Security", „Vernetzte Systeme", „Technisches Management") werden noch in den kommenden Jahren eingeführt. Beim Bachelor-Studiengang „IT und Telekommunikation" wird heuer neu ein „Kompetenzteam IT-

Die FH IT-Studiengänge auf einen Blick

WIEN

FH Technikum Wien www.technikum-wien.at
Bachelor:
- Elektronik
- Elektronik/Wirtschaft
- Informatik
- Informations- und Kommunikationssysteme
- Wirtschaftsinformatik

Master:
- Embedded Systems
- Informationsmanagement und Computersicherheit
- Multimedia und SW-Entwicklung
- Telekommunikation und Internet-Technologien
- Wirtschaftsinformatik
- Game Engineering und Simulation (ab WS 2008)

FH Campus Wien www.fh-campuswien.ac.at
Bachelor:
- Informationstechnologien und Telekommunikation
- Angewandte Elektronik
- Integriertes Sicherheitsmanagement

Master:
- IT-Security (ab 2009/10)
- Vernetzte Systeme (ab 2009/10)
- Technisches Management (ab 2010/11)

FH des bfi www.fh-vie.ac.at
Bachelor: Projektmanagement und Informationstechnik
Master: Projektmanagement und Organisation

Burgenland

FH Burgenland www.fh-burgenland.at
Bachelor:
- Informationsberufe
- Internettechnologien

Master:
- Angewandtes Wissensmanagement
- IT-Security (ab 2009/10)
- Information and Communication Solutions (ab 2009/10)

Niederösterreich

FH St. Pölten www.fh-stpoelten.ac.at
Bachelor:
- Communications & Simulation Engineering
- IT-Security
- Medientechnik

Master:
- Communications & Simulations Engineering (ab 2010/11)
- IT-Security (in Entwicklung)
- Telekommunikation & Medien (2007 neu)

FH Wiener Neustadt www.fhwn.ac.at
Bachelor: Informationstechnik
Master: Informationstechnik (2007 neu)

FH Krems www.fh-krems.ac.at
Bachelor: Unternehmensführung und E-Business-Management
Master: Unternehmensführung und E-Business-Management (ab 2008/09)

Steiermark

FH Joanneum www.fh-joanneum.at
Bachelor:
- Informationsmanagement (seit 2006, vorher Diplom)
- Informationsdesign (seit 2005, vorher Diplom)
- Internettechnik und -management (seit 2006, vorher Diplom)
- Health Care Engineering (seit 2006, vorher Diplom)
- Software Design (seit 2006, vorher Diplom)

Master:
- Advanced Security Engineering (seit 2006)
- IT-Recht und -Management (ab 2009/10)

Fachhochschulrat www.fhr.ac.at

Security“ eingebunden. Der Schwerpunkt liegt dabei auf abhör- und manipulationssicherer Datenübertragung.

„Wir erreichen dadurch neben dem Know-how-Zuwachs auch eine deutliche Qualitätsverbesserung und einen vermehrten Praxisbezug in der Lehre“, hofft Studiengangsleiter Johannes Walzer die positiven Faktoren gut nutzen zu können. Beim Bachelor „IT und Telekommunikation“ besteht zudem die Möglichkeit, sich aus den drei Bereichen „Angewandte IT-Sicherheit“, „Web-Engineering“ sowie „Telekommunikation“ einen Studienschwerpunkt zu wählen. Insgesamt hat die FH Campus Wien mit 207 Inskribierten (davon 23 Frauen) im IT/TK-Bereich deutlich weniger Studenten als das Technikum, das allerdings auch schon zehn Jahre länger besteht.

Von der EU gut bewertet

Die Wiener haben es gut: Es gibt sogar noch eine dritte Fachhochschule vor Ort: Die FH des bfi bietet seit dem WS 2001/02 den FH-Studiengang „Projektmanagement und Informationstechnologie“ (PIT) an. Jährlich beginnen je 45 StudentInnen sowohl in der Vollzeit als auch berufsbegleitend. „Bei uns können sich PIT-Studenten in den zwei Bereichen Digitale Medien und Medieninformatik spezialisieren“, sagt Studiengangsleiter Christian Malus. Die Umstellung vom alten Diplomstudium auf das Bachelor-Master-System erfolgte schon 2006. Nach dem 6-semestrigen Bachelor kann noch das Master-Studium „Projektmanagement und Organisation“ angeschlossen werden, das dann nochmals drei Semester dauert. Der Master wird nur berufsbegleitend angeboten.

Die FH des bfi erhielt letztes Jahr als einzige österreichische Hochschule das ECTS-Label („European Credit Transfer System“) von der EU-Kommission verliehen. Dieses Label führen außerdem nur die TU Graz und die FH Vorarlberg in Österreich. Mit der ECTS-Auszeichnung wird die internationale Ausrichtung anerkannt. Auslandssemester und Praktika werden an der FH problemlos angerechnet und in das reguläre Studium integriert.

Frauenanteil IT-TK-Studien

Technikum Wien:	9%
Campus Wien:	12,5%
FH des bfi:	27%
FH Wiener Neustadt:	11%
FH St. Pölten:	30%
FH Krems:	40%
FH Joanneum:	25-35%
FH Burgenland:	50%

(Zahlen laut Eigenangabe der jeweiligen FH)

Gute Chancen in NÖ

Freude herrscht auch in Wiener Neustadt. 50% mehr Studierende als im Vorjahr starteten im September ihr Bachelor- oder Masterstudium an der dortigen FH (1.100 Neuimmatrikulierte). Im Bereich IKT bietet die FH Wiener Neustadt bereits seit 1994 den Studiengang „Informationstechnik“ an, der im Moment von 101 Studenten absolviert wird.

„Mit dem Security-Angebot zählen wir zu den Ersten in Österreich.“ - **Sonja Gögele**, FH Joanneum, IT-Studiengangsleiterin am Standort Kapfenberg

Im Herbst wurde jetzt auch ein Master-Studiengang Informationstechnik gestartet, „hier bieten wir die Spezialisierungen Technische Informatik und Geoinformatik an“, erklärt Studiengangsleiter Martin Staudinger. Der erste Durchgang Bachelor ist schon vollendet, im Sommer 2007 konnten sich die ersten Informationstechnik-Bachelor über ihren Studienabschluss in Wiener Neustadt freuen, einige von ihnen setzen ihre Ausbildung mit dem neuen Master-Studium fort.

St. Pölten mit neuem Campus

Auch in St. Pölten ist man hoch motiviert. Der neueröffnete Campus erfreut sowohl die Lehrenden als auch die Lernenden. Die FH hat sich auch intern eine neue Organisationsstruktur zugelegt. Es gibt drei Departments: Medien & Wirtschaft, Soziales & Gesundheit sowie IT & Medien. Konnte ursprünglich in St. Pölten nur Medientechnik studiert werden (seit 1996) so stehen jetzt auch zwei weitere Bachelor-Studiengänge (Communications & Simulation Engineering und IT-Security) zur Wahl. Im Bachelor Medientechnik können jetzt die Vertiefungen „Audio/Video“ sowie „Interaktive Medien“ gewählt werden. Der erste Bachelor-Durchgang ist im Sommer fertiggeworden, daher steht ab diesem Wintersemester auch der (darauf aufbauende) neue Master-Studiengang Telekommunikation & Medien zur Verfügung.

„IT-Security wird im Moment stark nachgefragt.“ - **Alois Frotschnig**, FH St. Pölten, Leiter des Departments für IT & Medien

IT-Security ist „im Moment wahnsinnig nachgefragt und ein echter Renner“, stellt Alois Frotschnig, Leiter des Departments für IT & Medien, fest. Leider gibt es hier nur 30 Plätze. „Die Kombination aus Technik- und Management-Inhalten ist österreichweit einzigartig“, sagt er stolz. Für IT-Security wird gerade ein weiterführender Master-Studiengang entwickelt. „Die Studenten sind mit der Umstellung auf das neue Bachelor-Mastersystem sehr zufrieden“, stellt Frotschnig fest. Beratung und Service wird an der FH St. Pölten hochgehalten. Zweimal pro Jahr gibt es einen IT-Security-Day für Schüler mit Fachvorträgen und Labors. „Weiters bieten wir Schnuppertage und Workshops auch speziell für Schülerinnen an“, ist Frotschnig auch Information für künftige Technikerinnen ein großes Anliegen. Der Frauenanteil am IT und Medien Department in St. Pölten ist mit 30% allerdings schon ungewöhnlich hoch. „Der Grund dafür ist,

„Wirtschaftsinformatiker müssen die Welt der Informatik verstehen.“ - **Karl Ennsfellner**, FH Krems, Studiengangsleiter Unternehmensführung und E-Business-Management

„Wir erreichen neben dem Know-how-Zuwachs auch eine deutliche Qualitätsverbesserung und einen vermehrten Praxisbezug in der Lehre." - **Johannes Walzer**, FH Campus Wien, Studiengangsleiter IT und Telekommunikation

dass Medientechnik aufgrund des kreativen, gestalterischen Parts auch von vielen Frauen gewählt wird", erklärt Frotschnig.

Einen hohen Frauenanteil hat auch der Bachelor-Studiengang „Unternehmensführung und E-Business-Management" an der FH Krems. Das Studium wird seit 2001 in Vollzeit und seit 2002 auch berufsbegleitend angeboten und ist derzeit von 328 Studenten belegt. 50 Studienplätze werden pro Jahr vergeben. „Wirtschaftsinformatiker müssen die Welt der Informatik verstehen, dies wird durch Lehrveranstaltungen wie Einführung in die Programmierung, Konzeption und Gestaltung von Web-Seiten, Relationale Datenbanken, IT-Recht etc. gefördert", gibt Studiengangsleiter Karl Ennsfellner Einblick in den Lehrplan. Ab 2008/09 wird es dazu auch ein Master-Studium geben. „Der Fokus liegt dabei auf Unternehmensgründung und -übergabe sowie Leadership", erklärt Ennsfellner.

„Bei uns können sich PIT-Studenten in den zwei Bereichen Digitale Medien und Medieninformatik spezialisieren." - **Christian Malus**, FH bfi Wien, Studiengangsleiter Projektmanagement und Informationstechnologie

Graz und Eisenstadt

Breit gefächert ist das Angebot der renommierten FH Joanneum, die in Graz und Kapfenberg angesiedelt ist. Während „Informationsmanagement", „Informationsdesign" sowie „Health Care Engineering" in Graz angeboten wird, sind „Internettechnik und -management", „Software Design" sowie das noch sehr junge „Advanced Security Engineering"-Master-Studium in Kapfenberg angesiedelt. „Mit dem Security-Angebot sind wir mit Hagenberg die ersten in Österreich", ist Sonja Gögele, IT-Studiengangsleiterin in Kapfenberg, stolz auf die Pionierrolle. Leider gibt es im Moment nur 15 Plätze, „die Nachfrage war doppelt so groß", sieht Gögele ein großes Security-Interesse. „Pläne hätten wir noch viele, aber es gibt dafür kein Geld mehr", bedauert sie. „Wenn ich mir etwas wünschen könnte, dann, dass gegen das schlechte Image der Technik in der Gesellschaft in Österreich endlich etwas passiert", so Gögele kämpferisch. Sie schlägt z. B. verstärkt Image-Kampagnen für Naturwissenschaften bei 16-Jährigen vor.

Zufrieden mit der Entwicklung zeigt man sich im östlichsten Bundesland. An der FH Burgenland gibt es zurzeit 380 Studierende, davon die Hälfte weibliche (!), im Kernkompetenzbereich „Informationstechnologie und -management (es gibt insgesamt vier sogenannte „Kernkompetenzbereiche"). Neben zwei Bachelor-Studien und einem Master-Studiengang wollen die Burgenländer in zwei Jahren zusätzlich noch die zwei Masterstudiengänge „IT-Security" und „Information and Communication Solutions" einführen. „Internationalität wird bei uns in allen Bereichen gelebt, auch die Informationsmanager und IT-Techniker profitieren vom umfangreichen Netzwerk an internationalen Partnerhochschulen in ganz Europa", unterstreicht Sebastian Eschenbach einen der Vorzüge eines IT-FH-Studiums. Wer sparen muss, sollte sich ein Studium an den beiden letztgenannten FHs überlegen: Die FH Burgenland, die FH Joanneum (und die FH OÖ.) kosten den Studenten null Euro Studiengebühren, an allen anderen FHs (und Unis) sind 363 Euro Studiengebühren pro Semester fällig.

Derzeit beste Jobchancen

„Die Jobchancen sind enorm gut, vor allem Wirtschaftsinformatiker haben sofort einen Job", freut sich Helmut Gollner vom Technikum Wien. „Wir spüren, dass die Konjunktur anzieht", setzt Gollner hinzu. Die Studenten hätten jetzt das Glück, sich ihre Diplomarbeiten und Jobs aussuchen zu können.

„Der IT-Markt boomt, die Unternehmen brauchen einfach im Moment Personal", bemerkt auch Sonja Gögele von der FH Joanneum. „Projektmanager werden wieder stärker nachgefragt, vor allem die Mischung aus PM, IT und BWL stößt auf reges Interesse bei den Firmen", bestätigt Christian Malus von der FH des bfi Wien, der einen weiteren Effekt bemerkt, über den sich Absolventen freuen können: Die IT-Gehälter klettern zurzeit ordentlich in die Höhe.

Folge drei wird sich den IT-Studien an den Fachhochschulen in Oberösterreich, Salzburg, Kärnten, Tirol und Vorarlberg widmen.

(Porträt-Fotos von den FHs beigestellt)

IDC Green Day

IT und Umweltschutz
Wie kann IT zum Umweltschutz beitragen?
Wie "grün" ist Ihr Unternehmen?

IDC sieht Green IT als das **neue Top-Thema** und behandelt folgende Bereiche am Green Day:

- Virtualisierung und Konsolidierung
- verantwortungsbewusste Produktentwicklung, Produktion, Transport & Recycling von Hardware
- Next Generation Datacenters
- Change Management
- Nachhaltigkeit
- Corporate & Social Responsibility

Erfahren Sie am **IDC Green Day 2007**, wie Sie IT nachhaltig anwenden und damit Kosten sparen können!

Konferenz
28. November 2008
Architekturzentrum Wien, 1070 Wien

vmware HITACHI Inspire the Next IBM IDC Analyze the Future

IDC Central Europe GmbH - Niederlassung Österreich
Tel: +43 1 5267328 office@idc-austria.at
Fax: +43 1 5267329 www.idc-austria.at

Mit

Mit Energie kann man viel bewegen, für Wien und alle seine EinwohnerInnen genauso wie für den Sport. Als führender regionaler Energieversorger Österreichs leisten wir mit Strom, Gas und Fernwärme auch bei wichtigen Sport-Veranstaltungen unseren Beitrag für einen reibungs-

losen Ablauf. Mit WIEN ENERGIE bereit für sportliche Spitzenleistungen – damit ganz Wien in eine erfolgreiche Zukunft blicken kann. Nähere Informationen auf www.wienenergie.at

WIEN ENERGIE

TEIL UNSERER ZUKUNFT.

WIEN ENERGIE, ein Partner der EnergieAllianz Austria.

NetApp Innovation 2007

Storage-Hersteller Network Appliance lädt zur Storage-Konferenz ein

Es wird wieder Zeit für die NetApp Innovation. Das Topereignis der Storage-Branche findet heuer am 22. November im Vösendorfer Trend Eventhotel Pyramide statt. Der anerkannt größte Event dieser Art in Österreich versammelt erneut das *Who's Who* der Storage-Branche und bietet seinen Besuchern einen aktuellen Querschnitt des Storage- und Datenmanagements.

Daten speichern, verwalten, sichern und archivieren ist ein Themenkomplex, mit dem heute buchstäblich jede Unternehmung konfrontiert ist. Keine Daten - kein Business, könnte der kurze Nenner lauten. Network Appliance, bekannt als Hersteller von Datenspeicherlösungen vom Enterprise- bis zum KMU-Segment, hat mit der NetApp Innovation eine Konferenz ins Leben gerufen, die in kompaktem Format den Stand der Technologien und Lösungen beleuchtet. Das Aufgebot an Partnern aus Industrie und Fachhandel ist erneut beachtlich und trägt zum breiten Themenspektrum der Veranstaltung bei, bei der auch das Vergnügen nicht zu kurz kommt. Der Kärntner Kabarettist Manfred Tisal alias „Der EU-Bauer" wird den geselligen Teil des Tages einleiten. Tisals Büttenreden sind legendär. Man darf also auf die Ausführungen zur Hightech-Branche gespannt sein.

Umfangreiches Programm

Hightech vom Feinsten wird den Besuchern mit Eröffnung der Fachausstellung ab 9.00 Uhr geboten. Das Programm ist variabel gestaltet, sodass sich die Besucher die für sie relevanten Themen aussuchen können: Plenumsvorträge am Vormittag, parallel ablaufende Live-Demos und Workshops am Nachmittag oder einfach nur der Besuch der Ausstellung. Effizientes und sicheres Datenmanagement ist für viele Unternehmen eine Herausforderung und so gesehen genau richtig als Thema für die Eröffnungsrede. Die Konsolidierung von Daten und Storage ist dabei nur die Voraussetzung. Die erfolgreiche Praxis wird unmittelbar danach in

einem Kundenvortrag aufgezeigt. Redner von Brocade, Fujitsu Siemens Computers, VMware und NetApp befassen sich mit Kostenoptimierung, Hochverfügbarkeit im Rechenzentrum, Virtualisierung und Datenschutz.

Live-Demos und Workshops

Tiefer in die Technik geht es bei den Live-Demos und Workshops. Die Bandbreite der Themen von APC, Bull, NetApp, NTP, Riverbed und SupportEDV/Symantec ist groß und reicht von der Planung eines effizient organisierten Datenzentrums bis zu revisionssicherer Archivierung. Daten-

Die Teilnahme an der Veranstaltung ist für die Besucher kostenlos. Detaillierte Informationen und die Anmeldungsunterlagen unter www.netapp-innovation.at

wiederherstellung auf Knopfdruck, Lösungen für kleine und mittlere Unternehmen, Wege aus der Datenflut und schneller Datenzugriff für Filialbetriebe nach einer Storage-Konsolidierung runden das Nachmittagsprogramm ab und bieten den Teilnehmern reichlich Diskussionsstoff.

„Das große Interesse der Sponsoren, Partner und Kunden zeigt uns, dass wir mit der Struktur und den Inhalten dieser Storage-Konferenz richtig liegen. Nicht umsonst haben wir die Unterstützung von mehr als 25 Technologie- und Vertriebspartnern gewonnen. Für die Besucher der NetApp Innovation wird sich der Weg nach Vösendorf mit Sicherheit lohnen." - **Ewald Glöckl**, Country Manager Austria bei NetApp

Die NetApp Innovation ist für IT-Profis aus Unternehmen jeder Größe konzipiert, bietet aber auch einen Präsentationsrahmen für den Fachhandel. In der begleitenden Fachausstellung präsentieren NetApp-Partner ihr Software-, Lösungs- und Schulungsangebot inklusive Live-Demos. ❏

NetApp | NetApp Innovation

Weltweit den Maßstab für eine robuste Netzwerkinfrastruktur setzen

Immer mehr Organisationen suchen nach robusten Netzwerkinfrastrukturen, die sich für die vielfältigen IP-Anwendungen der Zukunft eignen.

Das geeignetste Verkabelungsmaterial, das der Markt zu bieten hat, stammt von Nexans. Es basiert auf Kategorie-7-Komponenten wie Kabel und die zugehörigen GG45-Steckerverbinder. NEXANS hat mit diesen modernen Komponenten weltweit viel Erfolg. So hat z. B. das EU-Parlament in Brüssel und in Luxemburg diese Baureihe als das zukunftssicherste System gewählt. Aber auch die deutsche DKV (Krankenversicherung) fand, dass dieses System auf die Dauer am zuverlässigsten und günstigsten ist. Einer der neueren Großkunden ist IKEA in Kuwait.

Ein österreichisches Unternehmen, das sich für die GG45-Technologie entschieden hat, ist die Firma Blaguss-Reisen. Blaguss schloss sich der internationalen Kooperation von mehr als 35 europäischen Busunternehmen namens „EUROLINES" an und errichtete den neuen, zentral gelegenen „VIB, Vienna International Busterminal". Dieser Busbahnhof wurde unter einem Teilabschnitt der Wiener-Stadtautobahn angesiedelt und ist mit der U-Bahn erreichbar.

Für den IT-Verantwortlichen bei Blaguss, Herr H. Jäger, ist die Technologie der GG45-Steckerverbinder besonders wichtig, da die neue Infrastruktur nicht nur für 10 Gigabit Ethernet geeignet ist. Die technischen Reserven reichen noch weit in die Zukunft und das verschafft die Sicherheit, auch für kommende Anforderungen bereits gerüstet zu sein. Ein sehr wichtiger Aspekt war auch, dass nexanszertifiziertes Montage-Personal zum Einsatz kam und damit eine 25-jährige NEXANS-Garantie erwirkt wurde.

„Ein Hauptpunkt, warum wir uns für den GG45 entschieden haben war, dass er rückwärtskompatibel ist und mit den vorhandenen RJ45-Patchkabeln zusammenpasst. Wir müssen in zukünftigen Anwendungen über 10G nur das Patchkabel wechseln und nicht die gesamte Infrastruktur", so Jäger.

„Schließlich wollen wir uns weder in der Datenübertragung noch bei Videoüberwachung, VoIP, Anzeigetafeln, der Bus-Waschanlage etc. Ausfälle leisten. Während der Umsetzungsphase hat uns der österreichische NEXANS-Distributor, die Kontakt-Systeme Inter, bestens unterstützt."

KSI

Kontakt-Systeme Inter Ges.m.b.H.
A-1230 Wien, Richard-Strauss-Str. 39
Tel.: +43/(0)1/61096-0
E-Mail: ksi@ksi.at
www.ksi.at

PROMOTION

Core-Switch

ProCurve Networking by HP stellt einen neuen Hochleistungs-Core-Switch mit passendem WLAN-Service-Modul vor.

Highend Core-Switch für Enterprise-Kunden

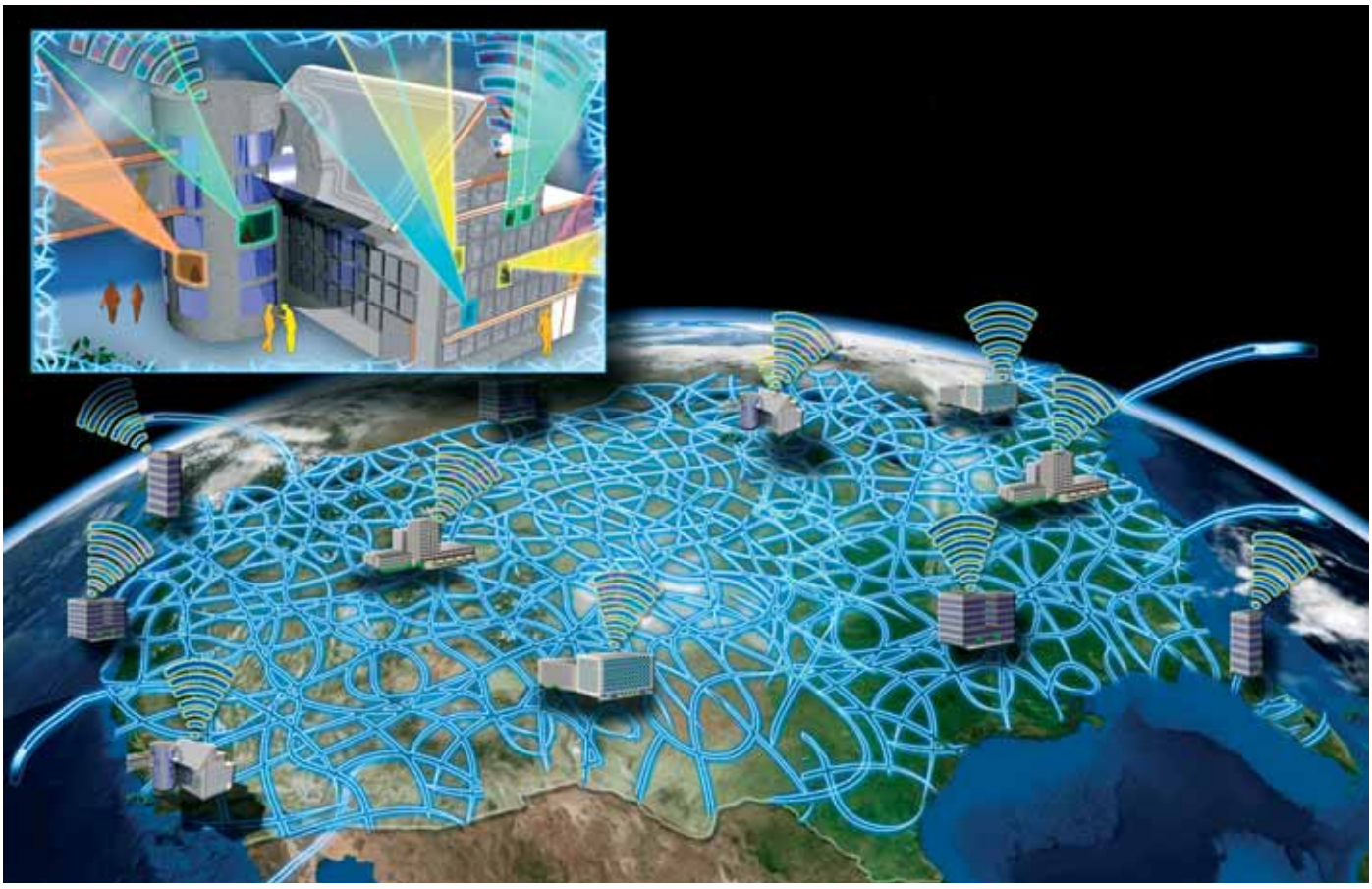
Der ProCurve Switch 8212zl wurde speziell für Enterprise-Kunden konzipiert und basiert auf der von HP entwickelten Pro Vision ASIC-Technologie. Damit vervollständigt ProCurve sein Portfolio für „Core-to-Edge"-Netzwerklösungen, die Netzwerk-Technologie, -Infrastruktur, -Software, -Betrieb, -Management als auch Support vereinen.

Der ProCurve Switch 8212zl ist eine Plattform für chassisbasierende Core-Switches. Sie bietet umfangreiche Layer-2- bis Layer 4-Funktionen sowie erweiterte Sicherheitslösungen. Mit hoher Gigabit-Dichte und einer 10-Gigabit-Konnektivität ist sie für besonders schnelle Anwendungen im Netzwerkkern geeignet. Redundanz bei Management und Stromversorgung sowie die Hot-Swap-Funktion ermöglichen eine verbesserte Netzwerkleistung, Systemstabilität und Hochverfügbarkeit.

Das ProCurve Wireless Edge Services zl-Modul ermöglicht WLAN-Integration ins LAN, -Konfiguration, -Management und verbesserten drahtlosen Service für den neuen Core-Switch 8212zl sowie für die Edge-Switches der 5400zl-Familie.

„Mit Hilfe von ProCurves Adaptive-Networks-Vision können Unternehmen die Infrastruktur an ihre Geschäftsanforderungen anpassen. Sie können schnell neue Anwendungen einführen, die Netzwerksicherheit erhöhen, die Produktivität steigern und die Komplexität reduzieren", ist John McHugh, Vice President und General Manager, ProCurve Networking by HP, überzeugt. Wie für die meisten ProCurve-Produkte gewährt das Unternehmen auch auf den 8212zl-Switch und das Wireless zl-Modul lebenslange Garantie. Beide neuen Produkte sind ab sofort verfügbar.
www.hp.com/at

Erwartungen an ein völlig neues Internet: Weitgehend unbekannte Wünsche erfüllen



Der Grundaufbau der GENI-Plattform für ein künftiges „Neues Internet" wird von einer auf optischen Technologien basierenden Basis getragen. Der Endnutzer wird vermutlich durch drahtlose Breitbanddienste angeschlossen (Grafik: Nicolle Rager Fuller, NSF).

Das GENI-Projekt nimmt in den USA die Arbeit auf

Dillan O. Klipstein

Das heutige Internet kommt in die Jahre. Seine Struktur macht es schwierig, neue Wünsche und Vorstellungen zu integrieren, die sich aus den praktischen Erfahrungen der vergangenen 25 Jahre ergeben haben. Das World Wide Web Consortium (W3C) in Cambridge (Massachusetts) weiß davon ein Lied zu singen: Für den Kopf dieses Gremiums, Web-Erfinder Tim Berners-Lee, bedarf es schon erheblichen Standvermögens, die vielfältigen Wünsche seitens der Anwender in geordnete Bahnen zu lenken. Denn bei allen Öffnungsbestrebungen für neue Dienste kann an der Grundstruktur nichts geändert werden, ohne das Ganze zu gefährden. Das neue Web 2.0 und noch mehr das künftige Web 3.0 haben mit dem Ur-Web nur die Basis gemeinsam.

Diese Erfahrungen sind auch an der National Science Foundation (NSF) nicht vorüber gegangen. Im Frühjahr 2005 hatte die NSF zu einem Workshop geladen. Ein Arbeitsteam um den Princeton-Professor Larry Peterson kam zu dem Ergebnis, dass man eine neue Forschungsplattform schaffen sollte für ein Internet des 21. Jahrhunderts: Die Idee des GENI (Global Environment for Network Innovations, http://geni.net) war geboren. Schnell war man sich im Klaren, dass die Basis eine dynamisch sich verändernde optoelektronische Ebene wäre, ergänzt durch Knoten, große Datenspeicher und ganze Cluster von Prozessoren sowie drahtlose Sub-Netze zum Endverbraucher: Alles das wurde als „GENI-Substrat" bezeichnet.

Wie man GENI zum Laufen bringt

Die NSF sieht sich als Impulsgeber und Mitfinanzierer. Im GENI Science Council (GSC) arbeiten Spitzenforscher aus Computer- und Netzwerktechnik zusammenarbeiten. Doch bei einer solch riesigen Aufgabe ist es mit einem Beratergremium nicht getan: Man braucht ein Projektbüro, in welchem die Fäden zusammenlaufen. Für die Leitung dieses GENI Project Office http://gpogeni.net brauchte man einen Kopf, der über entspre-

chenden Hintergrund verfügt. Und diesen Kopf hat man nun gefunden: Chip Elliott.

Wer ist Chip Elliott? Selbst Insider kennen ihn kaum: Er kommt von BBN, die in den vergangenen 50 Jahren an der Spitze vieler Technologieentwicklungen standen, insbesondere wenn es um regierungsnahe Entwicklungsaufgaben ging. Das Unternehmen wurde 1948 gegründet von den beiden MIT-Professoren Richard Bolt und Leo Beranek sowie dem ehemaligen Bolt-Studenten Robert Newman unter dem Firmennamen Bolt, Beranek & Newman, später abgekürzt BBN. Das Unternehmen hat seinen Sitz gleich um die Ecke vom MIT und ist wegen der Nähe zu seinen Auftraggebern auch in Washington vertreten (www.bbn.com). BBN gilt als einer der Pioniere für das seinerzeitige ARPANET, welches die Keimzelle und der Vorläufer des heutigen Internets war. Eine andere Entwicklung unter wesentlicher (Computer-)Beteiligung von BBN war Anfang der 80er-Jahre das Advanced-Land-Vehikel von Martin Marietta, das erste selbständig navigierende Fahrzeug. Es war Vorbild für den heutigen MarsRover.

So wie in dem vergangenen Vierteljahrhundert das Internet von einem fast obskuren Netzwerk der Forscher zu einem kritischen Stück der nationalen IT-Infrastrukturen wurde, so müsste heute aus den genannten Basisbausteinen ein neues Netz gezielt erarbeitet werden, dass die Erfordernisse der Zukunft erfüllen kann. Das ist we-

Tim Berners Lee, heute Chef des W3C-Konsortiums auf dem MIT-Campus in Cambridge (MA), hat sich während seiner Zeit am CERN in Genf sicher nicht vorgestellt, heute der Oberaufseher des World Wide Web zu sein.

der in ein paar Monaten zu erforschen, geschweige denn zu realisieren. Und es könnte für Elliott zu einer Daueraufgabe werden, wie es mittlerweile für Berners-Lee im 3WC ist: Auch der hat sich seinerzeit, als er noch bei der CERN in Genf war, nicht träumen lassen, die „Web-Spielerei" nun als Kopf einer bedeutenden Organisation fortzuführen. Es ist eine gigantische Aufgabe, ein solches „Neues Internet" zu skizzieren, die Technologien zu definieren und zu entwickeln und für eine dauerhafte Nutzung adaptionsfähig zu halten.

Chip Elliott von der BBN in Cambridge wird erster Leiter des GENI-Office und soll in dieser Funktion die Arbeiten an einer Plattform für ein völlig neues Internet koordinieren (Bild: William McCartney, ShoeFly Studio).

Die Zukunft des Internets vorauszuahnen - eine Herausforderung

Eines ist sicher: Der neue durch GENI zu definierende Rahmen wird mehr als 25 Jahre halten müssen. Mit wachsender Größe des Internets wird es immer schwieriger werden, einen weiteren Neuanfang zu machen. Denn eine Erblast wird es immer mit sich herumtragen: Die Kompatibilität zum Vorgänger. Über solche Rückwärts-Kompatibilität sind viele Entwicklungen fast ins Schleudern gekommen: Eine einheitliche Weltnorm fürs Fernsehen zum Beispiel, eine gemeinsame digitale Plattform für Video-Aufzeichnung, oder der Zwang, über lange Zeiträume auf uralte Programmiersprachen Rücksicht nehmen zu müssen - kurz: Auch GENI wird sich Freiräume schaffen müssen, in man heute noch unbekannte Entwicklungen einpassen wird.

Chip Elliott hat das erkannt: „Man muss sich ein völlig neues Internet vorstellen, das aller Wahrscheinlichkeit nach physikalisch mit dem heutigen wenig gemeinsam hat. Wir müssen sicherstellen, dass diese nächste Stufe aus den besten Ideen entsteht."

Eine virtuelle Visualisierung mag das Einstiegsbild geben. Man sieht die klare Unterscheidung zwischen terrestrischem Festnetz und drahtlose Netzen. Diese verbinden ein-

Das Advanced Land Vehicle (ALV) von Martin Marietta Aerospace in Denver (CO) war das wohl erste Fahrzeug der Welt, welches sich selbstständig in einem Gelände orientieren konnte. Da zu dieser Zeit die Standard-Prozessoren noch vom Typ i386 waren, hatte BBN in Cambridge einen Spezialrechner beigesteuert, der in Echtzeit auf die sich verändernden Daten beim autonomen Fahren reagieren konnte (Bild: Martin Marietta).

erseits das nationale Netz in den transnationalen Raum via Satellit, andererseits den Endteilnehmer via WLAN (siehe Bildausschnitt). Über den von den erwähnten GENI-Substraten gestellten Netzteilen liegt eine Art Softwarerahmen, der die verschiedenen Arbeitsebenen der GENI-Substrate managt. In den Substraten laufen Hunderte und Tausende von Vorgängen zur gleichen Zeit, jeder in einer eigenen Ebene. Man muss sich das als riesige Software-Architektur vorstellen: Die Anwender des neuen Internets sollen sogar in ihm mitarbeiten können, um weitere Ideen für die Nutzung einzubringen und auszuprobieren. Unwillkürlich fällt einem da das LINUX-Betriebssystem ein, welches sich ebenfalls ständig durch Anpassung wandelt.

GENI wird modular aufgebaut sein, mit einer festgelegten Grundarchitektur sowie einem umfangreichen Satz definierter Interfaces. Gerade hier aber wird man mit Sorgfalt vorgehen müssen, um sich für neue, heute unbekannte Netzwerktechnologien und Anwendungen offen zu halten. ❑

Maxdata: Neue Strategie

Neues Produkt-Sortiment und erweiterter Vertrieb sollen PC-Hersteller Maxdata fit für die Zukunft machen.

Belinea o.line: Für Trendsetter

„Wir haben unser Produktsortiment umfassend erneuert und werden damit in völlig neue Marktsegmente vordringen", erläutert Maxdata-Österreich-Geschäftsführer Werner Schiessl. Künftig werden unter dem Label „Belinea" auch Notebooks verkauft, insgesamt drei Produktlinien sollen Komplettlösungen für Geschäfts- und Privatkunden bieten. Der Einzelhandel komme als neuer Vertriebskanal hinzu.

Das Unternehmen, das in den letzten eineinhalb Jahren einen straffen Restrukturierungskurs gefahren ist, möchte dadurch die Umsätze steigern und rasch wieder in die Gewinnzone zurückkehren. „Wir haben die Kosten bereits deutlich gesenkt und die Verluste mehr als halbiert", so Schiessl. Die österreichische Landesgesellschaft selbst schreibe seit seinem 13-jährigen Bestehen stets schwarze Zahlen.

b.line: Business Computing in klassisch-zeitlosem Design

Auf Zielgruppen abgestimmt

Mit der Neuausrichtung des Produktportfolios orientiert sich Maxdata noch stärker als in der Vergangenheit an den Bedürfnissen der einzelnen Kundengruppen. Jede der drei neuen Belinea-Linien ist auf die Anforderungen einer speziellen Zielgruppe ausgerichtet und hat ein eigenes, durchgängiges Design: vom Notebook über den Monitor, von der Maus bis zur externen Tastatur.

Die neuen Belinea-Notebooks sind bereits unter den Bezeichnungen o.line, b.line und s.line zunächst im Fachhandel erhältlich. „Mit den drei Produktgruppen bieten wir dem Anwender ein einheitliches, aufeinander abgestimmtes Design für alle IT-Produkte, die ihren Platz auf dem Schreibtisch haben", sagt Werner Schiessl.

Die drei Produktgruppen bieten:

- o.line: Belinea für neugierige Trendsetter in frischem Design,
- b.line: Business Computing in klassisch-zeitlosem Design,
- s.line: exklusive Highend-Geräte.

Unterschiedliche Ausstattungslevel innerhalb der Lines sorgen für eine weitere Abstufung.

Flexible Fertigung

Ebenfalls neu: Ab sofort können andere Unternehmen von der Fertigung der Maxdata-Gruppe profitieren. Das frühere Tochterunternehmen Maxdata Systeme GmbH mit Sitz in Würselen bei Aachen firmiert seit Mai als Manulogs Manufacturing and Logistic Services GmbH.

„Das umbenannte Unternehmen bewirbt sich weltweit um Aufträge für Assemblierungs-, Logistik- und Serviceleistungen", erläutert Schiessl. Es verfüge über modernste Fertigungstechnologien und hochqualifizierte Mitarbeiter. Eine Endfertigung und Verteilung von IT-Produkten von Würselen aus sei für viele Anbieter hochattraktiv, da dieser Standort im Herzen Europas ein sehr flexibles Reagieren auf Kundenwünsche ermöglicht.

Maxdata wäre in der Vergangenheit wiederholt von internationalen IT-Herstellern auf Assemblierungs- und Supply-Chain-Leistungen angesprochen worden. „Ab sofort können nun sämtliche Leistungen von Einkauf und Beschaffung im globalen Umfeld über Engineering und Assemblierungsleistungen bis hin zur europaweiten Logistik und After Sales Services über Manulogs bezogen werden", betont Schiessl.

In Würselen werden auch Flachbildschirme (TFT-Monitore) gefertigt. So könnten erhebliche Kosten gespart werden: Denn wer seine Displays im Wide-Format mit DVI-Eingang ab einer Zollgröße von 19 außerhalb Europas produzieren lässt, muss bei der Einfuhr hohe Zollgebühren entrichten.

Weiterführende Informationen gibt es auf der neuen Website
www.belinea.at

Neue Multifunktionsgeräte

Xerox hat sein Office-Portfolio ausgeweitet: Die neuen MFPs unterstützen die Open-Source-Entwickleroberfläche Extensible Interface Plattform (EIP).

Das WorkCentre 7675 ist das neueste Multifunktionssystem im Portofolio von Xerox

Die Extensible Interface Plattform (EIP) ist eine neue, offene Programmierplattform von Xerox. EIP basiert auf Standard-Webtools, ausgerichtet auf eine schnelle Programmentwicklung und die individuelle Anpassung zahlreicher Funktionen, an die Bedürfnisse der jeweiligen Nutzer oder Arbeitsgruppen.

Die neuen DIN-A3-Farb-Multifunktionssysteme WorkCentre 7300 sowie das WorkCentre 7675 sind die ersten Farbsysteme, die EIP nutzen können. Zusätzlich wurde die WorkCentre 5600-Serie vorgestellt, das bislang schnellste DIN-A3-Schwarz-Weiß-Bürosystem von Xerox. Auch die WorkCentre 5600-Reihe ist voll EIP-fähig.

Neue Einsatzmöglichkeiten

Laut Xerox führt der Weg von der reinen Hardware zum Lösungsangebot. MFPs werden zunehmend mit Applikationen verbunden. Mit EIP können serverbasierte Anwendungen über den Touch Screen oder das Benutzer-Interface des Multifunktionsgeräts bedient werden. Sie basieren auf Web-Standards wie HTML, CSS (Cascading Style Sheets), XML und JavaScript.

Das soll den Nutzern verschiedene Vorteile bieten - neben der Umwandlung von Papierdokumenten in digitale Daten lassen sich Workflows vereinfachen; das Editieren, Speichern und Weitergeben von Informationen wird erleichtert. Einige Tätigkeiten wie das Finden und Ausdrucken von Dokumenten können direkt am Gerät und ohne einen Computer erledigt werden. „Das Zusammenspiel zwischen EIP und den neuen WorkCentre-Systemen hat das Potenzial, die Rolle von Multifunktionssystemen völlig neu zu bestimmen“, ist Hans Radl, Business Manager Office und EIP-Experte von Xerox Austria überzeugt. „Xerox treibt nicht nur den Wechsel zum Farbdruck an - der Arbeitsplatz wird mithilfe von webbasierten Services neu definiert.“

Neue Produkte

Das WorkCentre 7675 ist das neueste Multifunktionssystem im Portofolio von Xerox. Es druckt bis zu 75 Schwarzweiß-Seiten und 50 Farbseiten pro Minute bei einer Auflösung von bis zu 2.400 x 2.400 dpi.

Im Basispreis ist bereits ein Softwarepaket zur Kostenkontrolle enthalten, das es ermöglicht, die Nutzung zu überwachen und beispielsweise Druck-Limits für bestimmte Nutzer einzurichten. Das System ist sowohl in Sachen Druckgeschwindigkeit als auch vom durchschnittlichen Druckaufkommen her auf Großunternehmen und zentrale Druckabteilungen zugeschnitten. In Kürze erhält das WorkCentre 7675 zudem die renommierte NIAP-Zertifizierung (National Information Assurance Partnership), ein international anerkannter Standard für die Datensicherheit von IT-Geräten.

Die Produktreihe WorkCentre 7328, 7335 und 7345 ist auf die Bedürfnisse von Anwendern in kleinen und mittleren Unternehmen sowie von Arbeitsgruppen ausgerichtet. Die Druckgeschwindigkeit beträgt je nach Modell zwischen 28 und 45 Schwarzweiß-Seiten, während 26 bis 35 Farbdrucke pro Minute im Ausgabefach landen.

Die neue Produktreihe WorkCentre 5600 umfasst sechs Geräte mit Geschwindigkeiten von 32 bis 87 Seiten pro Minute. Kombiniert mit einem maximalen Fassungsvermögen von 8.700 Blatt können die Systeme sowohl Standard-Printjobs aus dem Büroumfeld als auch hochvolumige Druckaufträge schnell und effizient abwickeln.

Zusätzlich bietet Xerox die Service-Modelle PagePack und eClick an, die auf kleine und mittlere beziehungsweise große Unternehmen zugeschnitten sind. Die Verträge decken neben den Verbrauchsmaterialien auch die Wartung ab. Durch die kalkulierbaren Kosten können Anwender ihre laufenden Dokumentenkosten besser kontrollieren und in den Griff bekommen. www.xerox.at

Universal-Ladegerät

Das Schnell-Ladegerät erkennt verschiedenste Akku-Modelle und ermittelt selbstständig, über welche Pins der Akku aufzuladen ist.

Universelles Schnell-Ladegerät

Akkus aus DVD-Kameras, MP3-Playern, Mobile Phones, PDAs und Digitalkameras haben die unterschiedlichsten Formen und die Ladepole können stirnseitig, oben, unten oder seitlich angeordnet sein. Das neue Universal-Ladegerät von ARP DATACON kann laut Herstellerangaben 99% aller Li-Ion und Li-Polymer (3,6 V / 7,2 V) aufladen.

Die Konstruktion erlaubt es, die Kontakt-Pins nach links und rechts zu positionieren und sich somit an den jeweiligen Akku anzupassen. Die Kontakt-Pins lassen sich zudem um 90 Grad drehen, so dass auch Ladepole an der Ober- oder Unterseite des Akkus erreicht werden.

Die Bedienung funktioniert so: Akku einlegen, Kontakt-Pins positionieren, Kunststoffbügel einrasten und Strom einschalten. Ein Handy- oder Kamera-Akku wird nun in 1,5 bis 2,5 Stunden vollständig aufgeladen. Über farbige LEDs wird der Status des Ladevorgangs angezeigt. Ist der Akku aufgeladen, schaltet sich der Ladevorgang ab. Dank mitgelieferten Kabeln kann man das Universalgerät wahlweise an einer Steckdose oder im Auto verwenden.

www.arp.com

Neue Notebook-Familie

Fujisus Siemens Computers hat neue Einstiegs- und Midrange-Notebooks präsentiert.

Die Notebook-Serie mit dem Namen „Esprimo“ besteht aus den Serien U, M und D. Modell U9200 zeichnet sich mit seinem 12,1-Zoll-Display durch sein schlankes Design und das geringe Gewicht von 1,8 Kilogramm aus. Das ultra-portable Notebook ist vor allem für vielreisende Geschäftsleute konzipiert, die besonderen Wert auf Mobilität legen. Der M9400 mit 14,1-Zoll-Display ist mit einem Gewicht von 2,2 Kilogramm ebenfalls als Reisebegleiter gedacht.

Als Desktop-Replacement eignet sich der D9500 mit 15.4-Zoll-Display und 2.5 Kilogramm Gewicht. Alle Modelle sind, neben Wireless LAN, mit integriertem UMTS/HSDPA erhältlich. Mit zweiter Batterie ermöglichen die Esprimo Mobile Professional Notebooks laut Hersteller bis zu 8 Stunden Arbeiten ohne externe Stromzufuhr. Im Einstiegssegment ist ab sofort auch die V-Serie erhältlich (ab 549 Euro inkl. MwSt.).

www.fujitsu-siemens.at

Neue Fotodrucker

Canon bringt zwei neue Selphy-ES-Fotodrucker

Selphy ES2

Stressfreien Fotodruck ohne Computer verspricht Canon mit den neuen Selphy ES-Fotodruckern. Das Bild kommt über den PictBridge-Anschluss oder Speicherkarten-Steckplätze in den Drucker, auf dem großen Display kann man Bild- und Druckoptimierungsfunktionen auswählen. Optional steht eine Bluetooth-Schnittstelle bereit, der Selphy ES2 ist standardmäßig zusätzlich mit einer IrDA-Schnittstelle ausgerüstet

Beide Modelle arbeiten im Thermosublimationsdruckverfahren mit 256 Stufen pro Farbe und 16,8 Mio. Farben. Eine Schutzschicht sorgt für die bestmögliche Haltbarkeit der Prints. Easy-Photo-Packs in Form von All-in-One-Kassetten, kombinierten Farbband und Papier für bis zu 50 Fotoprints in einer Einheit. Es stehen unterschiedliche Formate wie Postkarten, Scheckkarten, Sticker zur Verfügung.

Der Selphy ES2 kommt auf ca. 209 Euro; der Selphy ES20 auf ca. 179 Euro. (UVP inkl. MwSt).

www.canon.at

19-Zoll-Display mit Lautsprecher

Benq präsentiert das 19-Zoll-Display E900 und das 17-Zoll-Display E700 mit integrierten Lautsprechern.

Beide Modelle aus der E-Serie eignen sich für den Arbeitseinsatz im Büro und zu Hause. Die Displays E900 und E700 sind mit dem Windows-Vista-Premium-Logo ausgezeichnet und verfügen über einen Kontrastwert von 800:1, eine Reaktionszeit von 5 ms sowie eine Helligkeit von 300 cd/m².

Die Bildschirme bieten einen Blickwinkel von 160 Grad vertikal und 160 Grad horizontal sowie eine Farbwiedergabe mit 16,7 Mio. Farben. Benq setzt dabei auf eine weiterentwickelte Technologie der Farbdarstellung über einen sRGB-Benutzermodus, der den Farbraum gemäß sRGB-Standards darstellt. Dadurch wird eine konsistente Farbwiedergabe auf dem Bildschirm ermöglicht, wenn weitere sRGB-kompatible Peripheriegeräte (Drucker, Digital-Kamera, Notebook etc.) an das Display angeschlossen werden.

Die BenQ-Monitore E900 und E700 sind zu einem empfohlenen Verkaufspreis von 239 Euro bzw. 209 Euro inkl. MwSt. im Handel erhältlich.

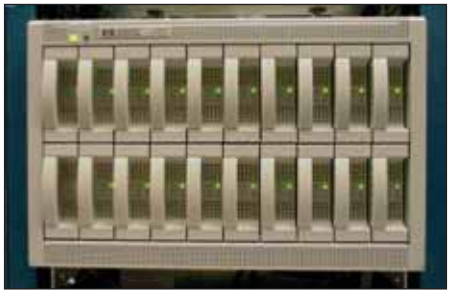
www.benq.at

Inserentenverzeichnis

ARP Datacon 37
Canon 5,7
cpsd 27
Data Systems Austria 23
Distrelec 61
Fujitsu Siemens 2.U
General Electric 36
IDC 53
Intersystems 49
ITdesign . . . . . .Cover Corner, 20, 25
Kaspersky 29
Kapsch 35
Kess Power Solutions 39
Kroll Ontrack 21
KSI 57
Maxdata 9
MGE USV 33
Microsoft 15
mii 20
mPAY24 59
mobil-data 43
Mobilkom 4.U
Rittal 31
Schmachtl 41
Schrack 35
Sicontact 21
Siemens Enterprise 45
SIGS . . . . . .Beilage
Triple AcceSSS IT 35, 37
Wien Energie 54, 55
Wiener Zeitung 11
WIFI 51

Vorschau auf Dezember 2007

Storage heißt heute nicht mehr, Daten nur einfach wegzuspeichern. Sie wollen nicht nur sicher verwahrt, sondern ebenso sicher wieder gefunden werden.



Ebenfalls in dieser Ausgabe: Branchen-Monitor „Öffenlicher Sektor“.

Allgemeine E-Mail-Adresse . . . . . office@monitor.co.at
Chefredakteur: Dipl.-Ing. Rüdiger Maier . . . . . maier@monitor.co.at
Redaktion: Mag. Dominik Troger . . . . . troger@monitor.co.at
Anzeigenleitung: Alexander Havlik . . . . . havlik@monitor.co.at
Anzeigenverkauf: Martina Gaye . . . . . gaye@monitor.co.at
Sekretariat: Hildegard Fatahtouii . . . . . fatahtouii@monitor.co.at
Technischer Leiter & Layout: Gerhard Hegedüs . . . . . hegedues@monitor.co.at

So erreichen Sie uns: Abohotline: 01-74095-466, E-Mail: abo.zv@bohmann.at
Monitor im Internet: http://www.monitor.co.at

Impressum

Medieninhaber und Verleger: Bohmann Druck und Verlag Ges.mbH & Co KG, Leberstr. 122, A-1110 Wien, Telefon 01/74095-410, Telefax 01/74095-425, E-Mail: office@monitor.co.at, www.monitor.co.at - **Chefredakteur**: Dipl.-Ing. Rüdiger Maier (mai) - **Redaktion:** Mag. Dominik Troger (dat) - **Autoren:** Peter Böhret, Conrad Gruber, Alexander Hackl, Peter Hanke, Adolf Hochhaltinger, Dillan O. Klipstein, Dunja Koelwel, Olaf Siemens, Ernst Tiemeyer, Dr. Christine Wahlmüller, Manfred Wöhrl - **Anzeigenleitung:** Alexander Havlik - **Technischer Leiter & Layout:** Gerhard Hegedüs - **Anzeigenverwaltung:** Hildegard Fatahtouii - **Aboverwaltung:** Bohmann Aboservice: Tel.:01-74095-466, E-Mail: abo@bohmann.at - **Druck:** Leykam Druck GmbH und Co. KG, Bickford Str. 21, 7201 Neudörfl. - **Verlags und Herstellungsort:** Wien - **Erscheinungsweise:** 11 x im Jahr plus drei Specials: „HARDWARE“, „SOFTWARE“, „KOMMUNIKATION“ - **Einzelverkaufspreise:** € 3,70 - **Monitor-Jahresabo:** € 33,20 - **Auslandsabo:** € 59,60 - **Anzeigenpreise:** Es gilt die Anzeigenpreisliste laut Mediadaten 2007 - **Bankverbindung:** Bank Austria Creditanstalt AG - Blz.: 12000, Kto.: 653 092 700, Österr. PSK - Blz.: 60000, Kto.: 1732.755 - DVR: 0408689 - FBNR: 9642f/FB - **Gericht:** HG Wien - **ARA Liz.-Nr.:** 1214 - UID ATU10940909 Für unverlangt eingesandte Manuskripte und Fotos wird keine Haftung übernommen. Die veröffentlichten Beiträge sind urheberrechtlich geschützt. Vervielfältigung, Nachdruck oder Übersetzung sind ebenso wie die Speicherung in Datenverarbeitungsanlagen und das bieten über Online-Dienste nur mit schriftlicher Genehmigung des Verlages erlaubt. Mit „Promotion“ gekennzeichnete Beiträge sind entgeltliche Einschaltungen.

ÖAK Auflagenkontrolle
Druckauflage 2. Quartal/2007: 14.500

PRESSE DOKUMENTATIONS NUTZUNG PARTNER

AKTIVIERUNGSENTGELT GESCHENKT*

A1 BREITBAND:

€20,– FÜR 3 GB

SURFEN SIE IM BESTEN NETZ – JETZT GÜNSTIG WIE NIE!

BLITZSCHNELLES INTERNET FÜR UNTERWEGS UND ZUHAUSE!

Nur bei A1 surfen Sie im besten und schnellsten Netz Österreichs**. Einfach anstecken und sofort lossurfen – kinderleicht! Jetzt so günstig wie nie zuvor***!

Shop nonstop mit €30,– ONLINE BONUS und weitere Infos auf www.A1.net

A1

TELE KOM AUS TRIA

* Bei Erstanmeldung zu A1 BREITBAND bis 03.11.07. ** Das IBK der TU Wien bestätigt beste dauerhafte Netzqualität und kürzeste Download- und Uploadzeiten für das Mobilfunknetz der mobilkom austria AG. *** Bei Erstanmeldung zu A1 BREITBAND 3 GB bis 31.01.08: minus €2,–/Monat auf das Grundentgelt von €22,– für die ersten 24 Monate. Mindestvertragsdauer 24 Monate. Rabatte bleiben bei der Berechnung eines etwaigen Restentgelts unberücksichtigt.